

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

JC398 U.S. PTO
09/309412
05/10/99



別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
in this Office.

出願年月日
Date of Application:

1998年 5月12日

出願番号
Application Number:

平成10年特許願第129214号

出願人
Applicant(s):

ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年 3月19日

特許庁長官
Commissioner,
Patent Office

伴佐山達志



【書類名】 特許願
【整理番号】 9800081404
【提出日】 平成10年 5月12日
【あて先】 特許庁長官 殿
【国際特許分類】 H04B 7/00
【発明の名称】 データ伝送制御方法及びデータ伝送システム
【請求項の数】 24
【発明者】
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内
【氏名】 原 和弘
【特許出願人】
【識別番号】 000002185
【氏名又は名称】 ソニー株式会社
【代表者】 出井 伸之
【代理人】
【識別番号】 100067736
【弁理士】
【氏名又は名称】 小池 晃
【選任した代理人】
【識別番号】 100086335
【弁理士】
【氏名又は名称】 田村 榮一
【選任した代理人】
【識別番号】 100096677
【弁理士】
【氏名又は名称】 伊賀 誠司
【手数料の表示】
【予納台帳番号】 019530

特平10-129214

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707387

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ伝送制御方法及びデータ伝送システム

【特許請求の範囲】

【請求項1】 通信経路を介してデータ送信手段からデータ受信手段に伝送するデータの伝送制御を行うデータ伝送制御方法において、

上記データ送信手段から上記データ受信手段へのデータの伝送に使用する第1の通信経路を介して、上記データ送信手段において暗号化されたデータを上記データ受信手段に送信し、

上記第1の通信経路よりもデータ伝送容量の小さく、上記データ受信手段から上記データ送信手段へのデータの伝送にも使用される第2の通信経路、及び上記第1の通信経路の内の少なくとも上記第2の通信経路を介して、上記データ送信手段から送信される上記暗号化されたデータを特定のデータ受信手段のみが受信するためのデータ限定伝送制御情報を上記データ受信手段に送信すること

を特徴とするデータ伝送制御方法。

【請求項2】 上記第2の通信経路は、上記データ送信手段と上記データ受信手段との間を双方向通信可能にする通信回線であること

を特徴とする請求項1記載のデータ伝送制御方法。

【請求項3】 上記データの暗号化は、上記データ送信手段におけるデータの暗号化を暗号鍵を用いて行い、当該データ送信手段から伝送された当該暗号化されたデータの上記データ受信手段における復号化を当該暗号化に使用した暗号鍵と同じ復号鍵を用いて行う共通鍵方式によること

を特徴とする請求項1記載のデータ伝送制御方法。

【請求項4】 上記暗号鍵及び上記復号鍵は、情報データを暗号化及び復号化するためのセッション鍵であること

を特徴とする請求項3記載のデータ伝送制御方法。

【請求項5】 上記データ送信手段及び上記データ受信手段は、データ受信手段固有のマスター鍵を有し、

上記データ送信手段は、上記マスター鍵を用いて上記セッション鍵を暗号化して、上記第1の通信経路又は上記第2の通信経路を経由させて上記暗号化したセ

ッション鍵を上記データ受信手段に伝送し、

上記データ受信手段は、上記マスター鍵を用いて、受信した上記暗号化されたセッション鍵を復号化して取り出すこと
を特徴とする請求項4記載のデータ伝送制御方法。

【請求項6】 上記データ送信手段は、特定の情報データの受信が許可される全てのデータ受信手段に対応させて上記セッション鍵を所持し、

上記データ送信手段は、上記特定の情報データの受信が許可されるデータ受信手段に上記セッション鍵を予め伝送しておくこと
を特徴とする請求項5記載のデータ伝送制御方法。

【請求項7】 上記第1の通信経路は、上記データ送信手段から上記データ受信手段への片方向通信のみ可能な衛星回線であり、

上記第2の通信経路は、データ送信手段とデータ受信手段の間で双方向通信可能な通信回線であること
を特徴とする請求項1記載のデータ伝送制御方法。

【請求項8】 暗号化を施してデータを送信するデータ送信手段と、
データ送信手段から上記暗号化が施されたデータが伝送されるデータ受信手段
と、

上記データ送信手段から上記データ受信手段へのデータの伝送に使用する第1
の通信経路と、

上記データ受信手段から上記データ送信手段へのデータの伝送にも使用され、
上記第1の通信経路よりもデータ伝送容量の小さい第2の通信経路と、
を有し、

上記データ送信手段から上記データ受信手段への暗号化したデータの伝送には
、上記第1の通信経路を用い、

上記データ送信手段から上記データ受信手段への当該データ受信手段から送信
する上記暗号化されたデータを特定のデータ受信手段のみが受信するためのデータ
限定伝送制御情報の伝送には、少なくとも上記第2の通信経路を用いること
を特徴とするデータ伝送システム。

【請求項9】 上記データの暗号化は、上記データ送信手段におけるデータの暗号化を暗号鍵を用いて行い、当該データ送信手段から伝送された当該暗号化されたデータの上記データ受信手段における復号化を当該暗号化に使用した暗号鍵と同じ復号鍵を用いて行う共通鍵方式によること

を特徴とする請求項8記載のデータ伝送システム。

【請求項10】 上記暗号鍵及び上記復号鍵は、情報データを暗号化及び復号化するためのセッション鍵であること
を特徴とする請求項9記載のデータ伝送システム。

【請求項11】 上記データ送信手段及び上記データ受信手段は、データ受信手段固有のマスター鍵を有し、

上記データ送信手段は、上記マスター鍵を用いて上記セッション鍵を暗号化して、上記第1の通信経路又は上記第2の通信経路を経由させて上記暗号化したセッション鍵を上記データ受信手段に伝送し、

上記データ受信装置は、上記マスター鍵を用いて、受信した上記暗号化されたセッション鍵を復号化して取り出すこと
を特徴とする請求項10記載のデータ伝送システム。

【請求項12】 上記データ送信手段は、特定の情報データの受信が許可される全てのデータ受信手段に対応させて上記セッション鍵を所持し、

上記データ送信手段は、上記特定の情報データの受信が許可されるデータ受信手段に上記セッション鍵を予め伝送しておくこと
を特徴とする請求項11記載のデータ伝送システム。

【請求項13】 上記第1の通信経路は、上記データ送信手段から上記データ受信手段への片方向通信のみ可能な衛星回線であること

を特徴とする請求項8記載のデータ伝送システム。

【請求項14】 通信経路を介してデータ送信手段からデータ受信手段に伝送するデータの制御を行うものであって、上記データ送信手段でデータを暗号化し、当該暗号化したデータを上記データ受信手段に上記通信経路を介して伝送するデータ伝送制御方法において、

上記データ送信手段から上記データ受信手段へ伝送するデータを複数のプロト

コルに応じて多重にカプセル化するとともに、少なくとも一つの上記カプセル化に対して暗号化を施すこと

を特徴とするデータ伝送制御方法。

【請求項15】 データのカプセル化は、上記データ受信手段への配信対象とするデータを第1のプロトコルに応じてカプセル化する第1のカプセル化工程と

上記第1のカプセル化工程においてカプセル化したデータを第2のプロトコルに応じてカプセル化する第2のカプセル化工程とにより行い、

上記第1のカプセル化工程は、上記データ受信手段への配信対象とするデータを全体を含む実データ部に当該実データ部に関する付加情報部を附加してカプセル化するとともに、上記実データ部については暗号化すること

を特徴とする請求項14記載のデータ伝送制御方法。

【請求項16】 上記付加情報部には、実データ部のデータの受信が許可されるデータ受信手段の宛先アドレス情報が含まれていること

を特徴とする請求項15記載のデータ伝送制御方法。

【請求項17】 上記データ送信手段は、当該データ送信手段においては情報データの暗号化に使用され、上記データ受信手段においては当該暗号化されて伝送してきた情報データの復号化に使用されるセッション鍵を上記宛先アドレス情報に対応して所持し、

上記データ送信手段は、上記セッション鍵を上記宛先アドレス情報により受信が許可されるデータ受信手段に予め伝送しておくこと

を特徴とする請求項16記載のデータ伝送制御方法。

【請求項18】 上記データ送信手段から上記データ受信手段への上記セッション鍵の伝送は、上記データ送信手段と上記データ受信手段との間を片方向又は双方向通信可能としている通信回線により行うこと

を特徴とする請求項17記載のデータ伝送制御方法。

【請求項19】 上記第1のカプセル化工程は、実データ部に附加される上記宛先アドレス情報の上記付加情報部への格納を一意に決定し、当該宛先アドレス情報に対応される上記データ受信手段固有のマスター鍵により実データ部を暗号

化すること

を特徴とする請求項15記載のデータ伝送制御方法。

【請求項20】 上記付加情報部には、上記宛先アドレス情報の格納用に48ビットの空間が用意されていること

を特徴とする請求項16記載のデータ伝送制御方法。

【請求項21】 上記第1のカプセル化工程により第1のプロトコルに応じてカプセル化されるデータは、インターネットプロトコル又はイーサネットプロトコルが採用されていること

を特徴とする請求項15記載のデータ伝送制御方法。

【請求項22】 通信経路を介してデータ送信手段からデータ受信手段に伝送するデータの制御を行うものであって、上記データ送信手段でデータを暗号化し、当該暗号化したデータを上記受信手段に上記通信経路を介して伝送するデータ伝送制御方法において、

暗号鍵を用いて上記データの上記暗号化を行うデータ暗号化工程と、
上記暗号化したデータに当該データの暗号化に使用した上記暗号鍵に関する暗号鍵情報を附加して、上記データ送信手段から上記データ受信手段へ送信するデータ送信工程と、

上記データ受信手段において受信した上記暗号化されたデータを復号するための復号鍵を複数有し、頻繁に更新される前記復号鍵から上記暗号化されたデータに付加されている上記暗号鍵情報に基づいて選択される一の復号鍵により、上記暗号化されたデータを復号化するデータ復号化工程と

を有すること

を特徴とするデータ伝送制御方法。

【請求項23】 上記複数の復号鍵は、受信される暗号化されたデータの復号化に現在利用可能とされる復号鍵及び受信される暗号化されたデータの復号化に次に使用される復号鍵であり、

上記データ復号化工程は、上記暗号鍵情報に基づいて上記現在可能な復号鍵を選択すること

を特徴とする請求項22記載のデータ伝送制御方法。

【請求項24】 上記暗号鍵及び上記復号鍵は、情報データを暗号化するためのセッション鍵であること

を特徴とする請求項23記載のデータ伝送制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信回線を利用してデータ送信装置からデータ受信装置へのデータの伝送の制御を行うデータ伝送制御方法及びデータ伝送システムに関し、詳しくは、データ送信装置から伝送されるデータの受信を特定のデータ受信装置に限定する制御を行うデータ伝送制御方法及びデータ伝送システムに関する。

【0002】

【従来の技術】

近年、データ送信装置から伝送されるデータを遠隔地に設置されている複数のデータ受信装置が受信可能とされるネットワーク型のデータ伝送システムが提供されている。例えば、衛星テレビジョン放送は、衛星回線を利用し、複数のデータ受信者に映像・音声情報を配信するいわゆるブロードキャスト的なデータ伝送システムを構築している。

【0003】

また、ブロードキャスト的なデータ伝送システムには、ローカルエリアネットワーク（LAN）として構築されるイーサネットが挙げられる。例えば、上記イーサネットのネットワークは、図14に示すように、データを送信するデータ送信装置351と、データ送信装置351からネットワーク353を介してデータが伝送されるデータ受信装置352a, 352bとから構成されている。例えば、このイーサネットにおいて、データ受信装置間の距離は、最大で数Kmまでとされている。

【0004】

このように構成されたデータ伝送システムにおいて、データ受信装置352aにデータを送信したい場合は、データ送信装置351は、ネットワーク353に向けてデータを送信する。この際、送信されるデータには、データ受信装置35

2 a を識別するための宛先アドレスが付加されて送信される。例えば、多くの宛先アドレスの情報を表現しようとした場合には、48ビット必要とされる。

【0005】

上記データ送信装置351からネットワーク353に送信されたデータは、データ受信装置352a及びデータ受信装置352bに受信され、各データ受信装置は、この受信したデータに付加されている宛先アドレスを参照して、自分宛のものであるかを判断する。例えば、イーサネットにおいて使用されるフレームフォーマットは、図15に示すように構成され、宛先アドレス (Destination Address) 401がデータの受信を行うデータ受信装置の宛先のアドレスを示す。

【0006】

ここで、データ受信装置は、判断の結果が自分宛でないと判断したとき、そのデータを破棄する。このような手続きによって、データに自己の宛先アドレスが付加されているデータ受信装置352aは、当該データを受信することができるが、データに自己の宛先アドレスが付加されていないデータ受信装置352bは、当該受信したデータを破棄することになる。

イーサネットにおけるデータ受信装置の受信処理は、図16に示すようなフローチャートに従って実行される。

【0007】

先ず、ステップS101において、データ受信装置は、ローカルエリアネットワークからデータが格納されたイーサネットフレームを受け取る。続くステップS102において、データ受信装置は、当該受け取ったイーサネットフレームから宛先アドレスを取り出す。そして、ステップS103において、データ受信装置は、宛先アドレスが自分宛てのアドレス（ユニキャストアドレス）又は自分が参加しているアドレス（マルチキャストアドレス）であるか否かを判別する。ここで、宛先アドレスが自分宛てのアドレス（ユニキャストアドレス）又は自分が参加しているアドレス（マルチキャストアドレス）であることを確認した場合には、データ受信装置は、当該イーサネットフレームをホストコンピュータに送信する。ここで、上記ユニキャストアドレスは、個人の宛先アドレスであって、上記マルチキャストアドレスは、複数のデータ受信装置が受信できるためのアドレ

ス、例えば、グループ単位でデータを受信するための宛先アドレスである。

【0008】

一方、宛先アドレスが自分宛てのアドレス（ユニキャストアドレス）又は自分が参加しているアドレス（マルチキャストアドレス）の何れでもないことを確認した場合には、データ受信装置は、当該イーサネットフレームを破棄する。

【0009】

上記宛先アドレスに基づいて行うデータの伝送方法によれば、標準通りに実装されたデータ受信装置であれば、宛先アドレスのないデータ受信装置は、データを受信することができないことになる。しかし、このようなデータ伝送方法においては、自己のアドレスを変更させるなどによりその判断機構を操作し、本来宛先アドレスとされていない、すなわちデータの送信対象とされていないデータ受信装置も他のデータ受信装置宛のデータを受信することが可能になり、これは他に知られたくないデータを送る際にはセキュリティの面で不安になる。

【0010】

だが、イーサネットにおいては、同じネットワークに接続されるデータ受信装置間の距離や台数が制限されており、他のデータ受信装置にデータの内容を知られて問題が起きる状況は少ないと考えられる。例えば、イーサネットの1つの形態である10BASE-5では、1つのセグメントのケーブルの長さは500mまでであり、そこに繋げられるトランシーバ（データ受信装置）の数は100台までと決められている。

【0011】

一方、上述した衛星回線によりデータ伝送のネットワークが構築された場合には、同一のネットワークが日本全国よりも広い範囲に渡って設置されることが有り得る。例えば北海道にあるデータ受信装置に送ったデータを、沖縄県にあるデータ受信装置が受信することも可能になる。このように、衛星回線によるネットワークでは、広範囲にデータを伝送し、さらにデータを受信可能とされるデータ受信装置の台数が多くなることから意図しない相手にデータを知られてしまう可能性が多くなる。

【0012】

よって、衛星回線などのブロードキャスト型の通信経路を用いてデータの伝送を行う場合には、データに何も加工を施さなければ、目的とするデータ受信装置以外のデータ受信装置においても、データの受信が可能になってしまう。この対策として、通信衛星を用いた現行のデジタル放送システムにおいては、送出するデータ（主に映像・音声情報）に暗号化を施してから衛星通信路上に伝送している。これに対応して、データ受信装置は、暗号化を解除する機能（復号化を行う機能）を有している。このようなデータ伝送方法により、予め視聴を許可されたデータ受信装置のみが復号化して視聴できるようになっている。これは、例えば、電気通信技術審議会74号答申に準拠した方式であり、伝送フォーマットとしてMPEG2（Moving Picture Experts Group Phase 2）のトランスポートストリームパケット（TSパケット）を用いている。例えば、データ送信装置におけるデータの暗号化は、暗号鍵を用いて行い、上記データ受信装置における復号化では、上記暗号鍵に対応される復号鍵により行う。上記TSパケットのフォーマットは、図17に示すように構成され、ヘッダ部のPID（Packet Identification）部411及びスクランブル制御部412により暗号鍵が特定される。ここで、例えば、暗号鍵は、セッション鍵Ksとワーク鍵Kwとがある。また、上記PID411は、13ビットのデータであり、上記スクランブル制御部412は、2ビットのデータである。

【0013】

上記TSパケットによりデータの伝送を行う既存の衛星テレビジョン放送におけるデータ伝送システムは、例えば、図18に示すように、データ送信装置501と、データ受信装置511とから構成されている。データ送信装置501は、各種暗号鍵により暗号化を行う暗号化ユニット502、503、504を有している。また、データ受信装置511は、各種復号鍵により復号化を行う復号化ユニット512、513、514と、資格判別ユニット515とを有している。

【0014】

このように構成されるデータ伝送システムにおいて、先ずデータ送信装置501からデータ受信装置511へのワーク鍵Kwの伝送が行われる。すなわち、上記

データ送信装置501は、上記P I D部411とスクランブル制御部412に対応したワーク鍵Kw506を予め作成する。そして、データ送信装置501は、当該ワーク鍵Kw506を、暗号化ユニット504において、マスター鍵507により暗号化し、データ受信装置511に伝送する。ここで、マスター鍵Kw507は、データ受信装置511固有のマスター鍵（復号鍵）518と同じ鍵とされている。データ送信装置501からデータ受信装置511への暗号化されたワーク鍵Kwの伝送は、衛星回線を経由して行われる。

【0015】

データ受信装置511では、マスター鍵Kw507により暗号化されたワーク鍵Kwを受信して、復号化ニット514において、当該データ受信装置511の固有のマスター鍵Km518により復号化する。そして、データ受信装置511は、復号して取り出したワーク鍵Kw517を上記P I Dと対応させて保存する。このワーク鍵Kwは、データ送信装置501から送信される暗号化されたデータの復号化に使用される。

【0016】

データ送信装置501からデータ受信装置511へのデータの送信については、上記データ送信装置501は、データのT Sパケットのペイロード部分413を、暗号化ユニット502においてセッション鍵Ks505により暗号化し、また同時に当該セッション鍵Ks505を暗号化ユニット503においてワーク鍵Kw506により暗号化する。

【0017】

データ受信装置511では、自分が復号可能なP I Dを持つT Sパケットを受信した際には、まず送られてきたT SパケットのP I D部411を見て予め保存してあった上記ワーク鍵Kw517を取り出す。そして、データ受信装置511は、データ送信装置501からデータと共に送信されてきた暗号化されたセッション鍵Ksをその取り出したワーク鍵Kw517を用いて復号化する。それから、データ受信装置511は、その復号化して取り出したセッション鍵Ks516を用いて、T Sパケットのペイロード部413を復号化し、データを取り出す。

【0018】

なお、視聴を許可されていないデータ受信装置にあっては、所定のワーク鍵Kwが送信されてきていないので、視聴したいP I Dに対応するワーク鍵Kwを所持することはない。よって、このようなデータ受信装置は、データ送信装置501から上記所定のワーク鍵Kwにより暗号化されて送信されてきたセッション鍵Ksを復号することができず、これにより、データ送信装置501から暗号化されて送信されてきたデータも復号することができない。よって、結局許可されていないデータ受信装置は、データを受信することはできるが復号化処理を行うことができないので、当該データを視聴できない。

【0019】

このようにして、衛星回線を用いた放送システムでは、限定的なデータの伝送制御を実現している。なお、上述したような、放送システムに限られず、例えば、インターネットにおいても様々な限定的なデータの伝送制御方法がある。

【0020】

例えば、インターネットに関しては、電子メールを暗号化して他者の盗聴や改竄を防ぐPGP (Pretty Good Privacy) 及びPEM (Privacy Enhanced Mail)、又はHTTP (Hyper Text Transfer Protocol) で電子商取引をする際などにクレジットカード番号を盗聴されないようにできるSSL (Secure Socket Layer) などが使われている。これらは暗号化方式を利用したり柔軟なデータ伝送制御ができることが特徴である。

【0021】

また、IP (Internet Protocol) データグラムに対するより汎用のデータ伝送制御方法として、認証ヘッダ (Authentication Header:AH) や、暗号ペイロード (Encapsulation Security Payload:ESP) などのIPSECと呼ばれる方式が標準化されている。

【0022】

【発明が解決しようとする課題】

ところで、衛星回線を使用したテレビジョン放送については、次のようなことが問題とされる。

【0023】

第1の問題点は、データ受信装置の限定範囲の種類が少ないことである。すなわち、暗号鍵を識別するための情報とされるP I D部及びスクランブル制御部が、図17に示すように、それぞれ13ビット及び2ビットしか用いていないため、最大でも15ビット分 ($2^{15}=32768$ 通り) の限定しかできない。

【0024】

第2の問題点は、利用するP I Dの数を増やすと、送信側のコストが増大することである。例えば、データ受信装置において、P I Dの数にほぼ比例した台数のM P E 2のエンコーダが必要になるため、P I Dの数を増加させると、それだけデータ送信装置のコストが増大し、装置が大掛かりなものになってしまう。

【0025】

第3の問題点は、衛星回線を利用したデータ伝送では、片方向の送信となるので、情報が各データ受信装置に正しく伝わったかどうかをデータ送信装置が知ることができない。これにより、例えば、データ受信装置がデータの受信を許可されているにもかかわらず、実際にはデータを受信することができないような事態が発生してしまう。だからといって、より確実に各種情報をデータ受信装置に送るには、時間が必要になり、これは、無駄が多く、柔軟なデータ伝送制御の妨げとなる。

【0026】

第4の問題点は、上述したように、I Pデータグラムを伝送する場合は、データ送信装置でインターネットプロトコルの宛先アドレスからP I Dの対応付けを行わなくてはならなく、インターネットプロトコルとの親和性に関して問題がある。具体的には、I Pデータグラムの宛先アドレスは32ビットあり、それよりビット長の短い13ビットのP I Dに対応付けるのは難しい等の問題がある。さらに、インターネットで現在用いられている上記の方法では、第5の問題点として、PGP、PEM、SSLなどは、アプリケーション固有のデータ伝送制御であり、インターネットでのすべてのアプリケーションで共通の方式ではないということである。アプリケーション毎に制御方法を用意しなくてはいけないので、新しいアプリケーションができたときへの素早い対応が難しくなる。

【0027】

第6の問題点としては、認証ヘッダや暗号ペイロードは、アプリケーションに依存していないが、既存のバージョンのインターネットプロトコル、例えばIP v4では対応しているネットワーク機器がほとんどないという問題がある。認証ヘッダや暗号ペイロードは、インターネットプロトコルの次期のバージョン、例えば、IP v6では標準的に利用されるが、既存のインターネットでは使うことは実質的に困難とされている。

【0028】

そこで、本発明は、上述の実情に鑑みてなされたものであり、データ送信装置からデータ受信装置へのデータの送信を安全に、さらに確実に行うことを実現可能にするデータ伝送制御方法及びデータ伝送システムの提供を目的とする。

【0029】

【課題を解決するための手段】

本発明に係るデータ伝送制御方法は、上述の課題を解決するために、データ送信手段からデータ受信手段へのデータの伝送に使用する第1の通信経路を介して、データ送信手段において暗号化されたデータをデータ受信手段に送信し、第1の通信経路よりもデータ伝送容量の小さく、データ受信手段からデータ送信手段へのデータの伝送にも使用される第2の通信経路、及び第1の通信経路の内の少なくとも第2の通信経路を介して、データ送信手段から送信される暗号化されたデータを特定のデータ受信手段のみが受信するためのデータ限定伝送制御情報を上記データ受信手段に送信している。

【0030】

このデータ伝送制御方法は、第1の通信経路を介して、データ送信手段からデータ受信手段へのデータの送信を行い、少なくとも第2の通信経路を介して、データ送信手段及びデータ受信手段の間でデータ限定伝送制御情報の送信を行う。

【0031】

このデータ伝送制御方法により、第1の通信経路及び第2の通信経路によりデータ送信手段からデータ受信手段へのデータ限定伝送制御情報を含むデータの送信を行うとともに、第2の通信経路により当該データ送信手段と当該データ受信

手段との間でのデータの送受信に関する情報に関して情報の交換を行う。

【0032】

また、本発明に係るデータ伝送システムは、上述の課題を解決するために、データ送信手段からデータ受信手段へのデータの伝送に使用する第1の通信経路と、データ送信手段と上記データ受信手段との間を双方向通信可能にする第2の通信経路とを有し、データ送信手段からデータ受信手段への暗号化したデータの伝送には、第1の通信経路を用い、データ送信手段からデータ受信手段への当該データ送信手段から送信する所定のデータを特定のデータ受信手段のみが受信するためのデータ限定伝送制御情報の伝送には、少なくとも第2の通信経路を用いる。

【0033】

このような構成を有するデータ伝送システムは、第1の通信経路を介して、データ送信手段からデータ受信手段へのデータの送信を行い、第2の通信経路を介して、データ送信手段及びデータ受信手段の間でデータ限定伝送制御情報の送信を行う。

【0034】

このデータ伝送システムにより、第1の通信経路及び第2の通信経路によりデータ送信手段からデータ受信手段へのデータ限定伝送制御情報を含むデータの送信を行うとともに、第2の通信経路により当該データ送信手段と当該データ受信手段との間でのデータの送受信に関する情報に関して情報の交換を行う。

【0035】

また、本発明に係るデータ伝送制御方法は、上述の課題を解決するために、データ送信手段からデータ受信手段へ伝送するデータを複数のプロトコルに応じて多重にカプセル化するとともに、少なくとも一つのカプセル化に対して暗号化を施す。

【0036】

このデータ伝送制御方法により、データ送信手段からデータ受信手段に送信されるデータが複数のプロトコルによって多重化されてカプセル化される。

【0037】

これにより、所定のプロトコルを保ったままデータの送信が可能になり、すなわち、例えば、所定のプロトコルとの互換性を保ったままデータの送信が可能になり、さらに、所定のデータを格納するための空間が確保することができるプロトコルによりカプセル化することにより、各種情報を格納するためのデータ空間が確保される。さらに、暗号化が施されることにより、データの安全性が保たれる。

【0038】

また、本発明に係るデータ伝送制御方法は、上述の課題を解決するために、暗号鍵を用いてデータの暗号化を行うデータ暗号化工程と、暗号化したデータに当該データの暗号化に使用した上記暗号鍵に関する暗号鍵情報を付加して、データ送信手段記からデータ受信手段へ送信するデータ送信工程と、データ受信手段において受信した暗号化されたデータを復号するための復号鍵を複数有し、頻繁に更新される前記復号鍵から上記暗号化されたデータに付加されている上記暗号鍵情報について選択される一つの復号鍵により、暗号化されたデータを復号化するデータ復号化工程を有する。

【0039】

このデータ伝送制御方法は、データ暗号工程において暗号鍵により暗号化されたデータに当該データの暗号化に使用した暗号鍵に関する暗号鍵情報を付加して、データ送信工程により、データ送信手段からデータ受信手段へ当該データを送信する。そして、データ受信手段において、データ復号化工程により、受信した暗号化されたデータを復号するための複数の復号鍵であって、頻繁に更新される復号鍵から、暗号化されたデータに付加されている暗号鍵情報について選択した一つの復号鍵により、当該暗号化されたデータの復号化を行う。

【0040】

このデータ伝送制御方法により、データ送信手段は、暗号鍵によるデータの暗号化を行い、データ受信手段は、受信した暗号化されているデータを復号鍵により復号化する。さらに、データ受信手段は、頻繁に変更される復号鍵から一の復号鍵を選択して、当該選択した復号鍵により復号化を行う。このとき、データ受

信手段は、当該暗号化されたデータとともに送信されてくる暗号鍵情報に基づいて複数の復号鍵から一つの復号鍵を選択する。

【0041】

【発明の実施の形態】

以下、本発明の実施の形態について図面を用いて詳しく説明する。この実施の形態は、本発明に係るデータ伝送システムを、衛星回線を介してデータ送信装置から伝送されるデータの受信を特定のデータ受信装置に限定する制御を行うデータ伝送システムに適用したものである。

【0042】

上記データ伝送システムは、図1に示すように、通信経路とされる衛星回線4a、専用線7、電話回線8、及び双方向の通信経路9を介してデータ送信装置2からデータ受信装置3a, 3b, 3cに伝送するデータの制御を行うものであって、上記データ送信装置2でデータを暗号化し、当該暗号化したデータをデータ受信装置3a, 3b, 3cに通信経路を介して伝送するデータ伝送システムである。

【0043】

このデータ伝送システム1は、データ送信装置2からデータ受信装置3a, 3b, 3cへのデータの伝送に使用する第1の通信経路とされる通信衛星4を利用した通信経路4aと、データ送信装置2とデータ受信装置3a, 3b, 3cとの間を双方向通信可能にする第2の通信経路である専用線7、電話回線8、及び双方向の通信経路9とを有している。そして、データ伝送システム1は、データ送信装置2からデータ受信装置3a, 3b, 3cへの暗号化したデータの伝送には、上記第1の通信経路を用い、データ送信装置2からデータ受信装置へのデータ限定伝送制御情報の伝送には、上記第2の通信経路を用いている。そして、データ伝送システム1は、インターネットと接続されている。

【0044】

ここで、データ限定伝送制御情報とは、上記データ送信装置2から送信する所定のデータを特定のデータ受信装置のみが受信するための情報である。すなわち、データ伝送制御情報とは、特定のデータ受信装置のみが所定のデータの受信が

許可されるための情報である。

【0045】

上記データ送信装置2は、上記各通信回線を利用してデータ受信装置3a, 3b, 3cへの各種データの配信を行う。データ受信装置3a, 3b, 3cは、各通信回線から伝送されてくるデータを受信する。なお、図1には、データ受信装置3a, 3b, 3cを3台として示しているが、実際には数百台から数万台のデータ受信装置が存在して当該データ伝送システム1を構成している。

【0046】

このデータ送信装置2とデータ受信装置3a, 3b, 3c（なお、以下の説明では、データ受信装置3a, 3b, 3cについて特定する必要がない場合には、単にデータ受信装置3という。）との間でデータの送受信を可能にする通信経路については、次のように構成されている。

【0047】

上記衛星回線4aは、約30Mbpsの帯域を持ったKuバンドの片方向の回線を想定する。この衛星回線4aにより、例えば、日本全国に分布されているデータ受信装置に対して、データ送信装置2からのデータの伝送を同時期に行うことができる。

【0048】

双方向の通信経路9は、データ送信装置2とデータ受信装置3との間で、衛星回線4aとは別に設けた通信経路であって、データ送信装置2とデータ受信装置3との間での双方向通信を可能にするものである。ここでは、双方向の通信経路9は、インターネットでの通信に用いる汎用の通信経路を想定している。

【0049】

専用線7は、データ送信装置2とデータ受信装置3とを直接接続している通信手段である。

【0050】

上記インターネット6は、いわゆる映像情報、音楽情報等の各種情報を提供するものであって、上記インターネットサービスプロバイダ5により、インターネット6とデータ受信装置3とは通信可能に接続されている。ここでデータ送信送

信装置2は、インターネット6に接続されている。

【0051】

なお、上述したようにデータ送信装置2とデータ受信装置3との間でデータの送受信を可能にする専用線7、電話回線8、及び双方向の通信経路9は、衛星回線4aほど大容量の帯域ではなく、数Kbpsから数百Kbps程度が通常の帯域とされる。

【0052】

上記データ伝送システム1は、所定のデータを特定のデータ受信装置においてのみ受信することを可能にするいわゆるデータ限定受信システムとしても構築されており、例えばデータ受信装置3aのみにデータを伝送するといった個別配信（ユニキャスト型データ配信）、又は例えばデータ受信装置3a, 3bとからなる受信グループにのみデータを伝送するといったグループ宛の同報配信（マルチキャスト型データ配信）、又は全てのデータ受信装置3a, 3b, 3cに同時にデータを伝送するといった一斉配信（ブロードキャスト型配信）等の配信形態が可能とされて構成されている。

【0053】

次に、このデータ伝送システム1において、データ送信装置2からデータ受信装置3へのデータの传送について説明する。データ送信装置2からデータ受信装置3へ传送されるデータは、図2に示すように、データのカプセル化が施されている。このカプセル化は、データを传送するデータ送信装置2において行われる処理であって、第1のカプセル化工程により、データ受信装置3への配信対象とされるデータを第1のプロトコルによりカプセル化し、第2のカプセル化工程により、上記第1のプロトコルによりカプセル化したデータを第2のプロトコルによってカプセル化する。ここで、カプセル化とは、データ自体に対して加工を施すことなく、当該データ自身を通信プロトコルにより規定された传送フォーマットに基づいて構成されるカプセル（パケット又はフレーム等）に入れ込むことをいい、このカプセル化によりデータの传送制御が可能になる。

【0054】

上記第1のカプセル化工程では、データ受信装置3への配信対象とするデータ

の全体を含む実データ部に当該実データ部に関する付加情報部を付加してカプセル化するとともに、上記実データ部については暗号化して上記カプセル化を行う。以下に詳しく説明する。

【0055】

IP (Internet Protocol) データグラム101は、図2中(a)に示すように、インターネットプロトコルに則して構成されているデータである。このIPデータグラム101は、上記データ受信装置3への配信対象とされるデータを格納して構成されている。そして、IPデータグラムのヘッダ部には、例えば、インターネット上において使用される宛先を識別するための送信先アドレス (Destination Address) が付加されている。

【0056】

なお、IPデータグラム101の部分は、インターネットプロトコルとして構成されることに限定されるものではなく、イーサネットプロトコルを採用して構成されてもよい。

【0057】

そして、データ送信装置2は、図2中(b)から図2中(d)に示すように、データを上記第1のプロトコルによりカプセル化する。例えば、第1のプロトコルとしては、DVB (Digital Video Broadcasting) のMultiprotocol Encapsulationを採用している。

【0058】

先ず、データ送信装置2は、第1のプロトコルによるデータのカプセル化を、図2中(b)に示すように、IPデータグラムに対してパディングを行い(パディング部102を付加する)、データ部の長さを64ビットの整数倍にする。例えば、IPデータグラム101の末尾に0ビット～63ビット長のパディングを行い、パディングするビットは、すべて1とする。このパディングにより、所定のデータ長さにすることができる、これは、上記セクションのデータ部を暗号化する際に、データ部の長さが64ビットの整数倍の方が都合が良いからである。以後、第1のプロトコルのフォーマットによって構成されるデータ部分をセクションと呼ぶことにする。

【0059】

次に、データ送信装置2は、パディング102が付加されたセクションを、図2中(c)に示すように、暗号化する。ここで、暗号化は、暗号鍵によって行うもので、暗号鍵は、上記データ受信装置3に対して配信の対象とされる情報について暗号化するために使用される後述するセッション鍵である。また、暗号化の方式としては、Triple-DESのような共通鍵方式のブロック暗号化を用いる。このTriple-DES方式の暗号化は、公開鍵方式の中でも強力な暗号方式であり、ハードウェアによる実装で高速化も容易とされる。これにより、30Mbps程度の高速な暗号化にあっても、公開鍵方式の暗号化とは異なり、処理時間がかかるデータの伝送が間に合わなくなることを防止することができる。

【0060】

そして、データ送信装置2は、図2中(d)に示すように、暗号化されたセクションデータ部104に、セクションヘッダ部103及びエラー検出のために使用されるテイラ部105を付加する。

【0061】

ここで、上記暗号化されたセクションデータ部104は、MAC(Media Access Control)フレーム化されて構成されている。このMACフレーム化により、データ部にMACヘッダが付加され、このMACヘッダ部を参照することにより、当該フレーム化されて格納されているデータの宛先の制御が容易となれるようになる。具体的には、MACフレームには、当該MACフレーム化されたデータの受信が許可されているデータ受信装置の宛先アドレスが格納されている。

【0062】

上記セクションヘッダ部103は、宛先アドレスを格納する部分であって、48ビットの宛先アドレスが格納されるようにデータ空間が確保されている。具体的には、上記セクションヘッダ部103においてMACヘッダ部を構成して、宛先アドレスが格納されている。このセクションヘッダ部103に48ビットにより表現される宛先アドレスを格納できる空間を設けることにより、上記第1の問題点とされていた、データ受信装置の限定範囲の種類が少ないと解消することができる。すなわち、暗号鍵を識別するための多くの情報を格納することができ

きるようになる。さらに、上記第4の問題点とされていた、IPデータグラム101を伝送する際に、インターネットプロトコルの宛先アドレスから後述するパケットIDの対応付けを行わなくもよくなり、インターネットプロトコルとの親和性を得ることができる。

【0063】

また、上記テイラ部105は、CRC (Cyclic Redundancy Checking、巡回冗長検査) によってコード化されている。CRCは、MACフレーム化されたデータを受信したデータ受信装置3が、当該MACフレームが正しく衛星回線において伝送されているかを検査するためのものである。例えば、CRCは、32ビットによってコード化されている。

【0064】

以上が第1のプロトコルによる配信対象とされるデータのカプセル化であって、次に、この第1のプロトコルによってカプセル化されたデータを、第2のプロトコルによってカプセル化させる処理について説明する。

【0065】

第2のプロトコルによるカプセル化は、上記第1のプロトコルによってカプセル化されたデータを、複数のパケットに分割することにより実行されるカプセル化である。ここで、第2のプロトコルは、TS (Transport Stream) パケット化によるものである。MPEG2 (Moving Picture Experts Group Phase 2) によって規格されているものであって、オーディオ、ビデオ信号やデータのような多種類のデータが多重化されて、大容量のディジタル回線で伝送することが可能になる。この第2のプロトコルにより、図2中(e)乃至図2中(g)に示すように、カプセル化されて、複数のTSパケット106, 107, 108に分割される。ここで、TSパケット106, 107, 108は、TSヘッダ部H_{TS}と、TSペーロード部Pとによって構成され、上記TSペイロード部Pには、分割されて上記第1のプロトコルによってカプセル化されたデータが格納される。そして、TSパケットのTSヘッダ部H_{TS}には、上記図17に示すような、パケットID (PID) 部及びスクランブル制御部によって構成される。なお、従来においては、このPID部及びスクランブル制御部に宛先アドレスが書き込んでいるこ

とにより、宛先アドレス情報が制限される等の問題があったが、本実施の形態においては、上述したように、宛先アドレスをセクションヘッダ部103に書き込むことにより、これを解消している。

【0066】

以上が第2のプロトコルによるカプセル化であり、よって、データ送信装置2は、データ受信装置3への配信対象とされるデータ（IPデータグラム）を第1のプロトコル及び第2のプロトコルによって多重にカプセル化して、通信衛星4への当該データの伝送を行っている。

【0067】

このように、TSパケットとセクションの2つのレベルにおいてそれぞれ独立なデータ限定伝送制御を行っているので、上記第2、第5、及び第6の問題点が解消される。

【0068】

すなわち、上記第2の問題点とされていた、利用するPIDを増加することなく、暗号鍵について多くの情報を確保することができる。

【0069】

また、上記第5の問題点とされていた、アプリケーション毎に制御方法を用意しなくて済み、新しいアプリケーションへの素早い対応ができるようになる。

【0070】

さらに、第6の問題点とされていた、認証ヘッダや暗号ペイロードを既存のインターネットで使うことができるようになる。

【0071】

なお、上述したようなIPデータグラムをカプセル化してデータ受信装置3に送信する方法は、衛星回線4aを介して行う際のものであり、双方向の通信経路9にあっては、特殊なカプセル化は行わず、通常のインターネットと同様の方式でIPデータグラムを伝送する。

【0072】

次に、データ送信装置2において行う暗号鍵によるデータの暗号鍵及びデータ受信装置3において行う暗号化されているデータの暗号鍵（復号鍵）による復号

化について説明する。ここで、データ送信装置2及びデータ受信装置3は、図3に示すように構成され、データ送信装置2とデータ受信装置3とは、上記図1に示すような通信経路により接続されている。ここで、データ送信装置2からデータ送信装置3へのデータ伝送を第1のプロトコル（セクション）において行い、従来として説明した上記図18については、本発明の実施の形態でいう第2のプロトコル（TSパケット）により行っている。すなわち、本発明実施の形態である図3と従来のものとされる図18とに示されるデータ送信装置及びデータ受信装置を比較すると、本発明に係る実施の形態とされるところのデータ送信装置とデータ受信装置において暗号化及び復号化に使用される鍵のレベル、すなわち、鍵の使用個数が1つ少なく、セッション鍵Ks24とマスター鍵Km25の2レベルになっている。

【0073】

ここで、セッション鍵Ks24は、上記データ送信装置2及び上記データ受信装置3が共に所持しているデータの暗号化／復号化に使用する鍵であり、いわゆる共通鍵方式が採用されている。なお、便宜的にデータ送信装置3が所持する方のセッション鍵Ksをセッション鍵Ks34とする。

【0074】

すなわち、データ送信装置2は、セッション鍵Ks24により、特定のデータ受信装置に対して送る情報データを暗号化する。また、データ受信装置3は、配信されてきた暗号化されたデータをセッション鍵Ks34により復号化して意味のある情報として取り出す。

【0075】

そして、セッション鍵Ks24, 34は、一定時間毎に更新される暗号鍵であって、例えば、日毎、時間毎、分毎に変化する。よって、ある時点でのセッション鍵Ks24を盗聴者が知ったとしても、有効とされる期間が一定期間であることから、そのセッション鍵Ks24により一定期間しかデータの盗聴をすることができない。このセッション鍵Ksの更新については、後述する。

【0076】

このセッション鍵Ks24により、図2内(c)に示すセクションのデータ部は

、上記Triple-DESにより暗号化される。

【0077】

マスター鍵Km25は、上記セッション鍵Ksと同様に、データ送信装置2及びデータ受信装置3が共に所持している暗号鍵であって、各データ受信装置3A, 3B, 3Cに固有のものである。なお、便宜的にデータ送信装置3側の所持するマスター鍵Kmをマスター鍵Km35とする。

【0078】

このマスター鍵Ks25は、データ送信装置2とデータ受信装置3と間を送信処理されるようなことはなく、すなわち、通信経路上に存在する場合ではなく、これによりいかなる手段によっても他人によって知ることができない暗号鍵とされている。

【0079】

このマスター鍵Kmは、セッション鍵Ksをデータ送信装置2からデータ受信装置3に送信する際に、セッション鍵Ksを暗号化／復号化するために用いられる。すなわち、データ送信装置2は、マスター鍵Km25によりセッション鍵Ks24を暗号化してデータ受信装置3に予め伝送しておく。データ受信装置3は、受信した暗号化されているセッション鍵Ks24を、当該データ受信装置3が所持しているマスター鍵Kmによって復号化して取り出す（セッション鍵Ks34として取り出す）。

【0080】

このマスター鍵Kmによる暗号化及び復号化により、セッション鍵Ksは、データ送信装置2からデータ受信装置3へ伝送する間に盗聴者が存在している場合であっても、知られるようなことはない。

【0081】

そして、データ受信装置3は、復号化したセッション鍵Ksにより、当該セッション鍵Ksにより暗号化されて伝送されてくる情報データの復号化を行い、情報データを意味のある情報として取り出す。

【0082】

なお、このマスター鍵Kmによるセッション鍵Ksの暗号化／復号化についても、

上記Triple-DESに基づいて行うが、公開暗号方式を採用することもできる。これは、公開暗号方式は、鍵の暗号化及び復号化がデータの暗号化/復号化とは異なり高速性を要求されないこと、安全性を確保することができるからである。

【0083】

また、マスター鍵Km25は、セッション鍵Ks24と異なり、時間と共に変化することはない。

【0084】

ここで、セッション鍵Ks24の変更について説明する。セッション鍵Ksの変更については、データ送信装置2が能動的に行うものとし、マスター鍵Km25で暗号化したセッション鍵Ks24（以下、マスター鍵Kmにより暗号化されたセッション鍵Ksを、暗号化されたセッション鍵Km(Ks)という。）の伝送もデータ送信装置2が能動的に行うものとする。

【0085】

また、双方向通信経路9を利用することにより、データ受信装置3の側から能動的にセッション鍵Ksの要求を行うこともできる。これにより、各データ受信装置3a, 3b, 3cは、素早く確実に必要なセッション鍵Ks24をデータ送信装置3から取得することができる。具体的には、新たにデータ受信装置3がこのデータ伝送システム1に加わる場合、障害によりこの系から外れていたデータ受信装置3が障害から復旧して再びこのデータ伝送システムに加わる場合、またデータ受信装置3においてセッション鍵Ksが正しく受信出来なかった場合には、データ受信装置3の側から能動的にセッション鍵Ksの要求を行うことにより、各データ受信装置3a, 3b, 3cは素早く確実に必要なセッション鍵Ks24を取得することができる。例えば、上述したような障害復旧やセッション鍵Ksの更新の管理は、データ送信装置2及びデータ受信装置3内にあるCA（Conditional Access）管理ユニット23, 33により行い、両者が双方向に通信を行って制御情報のやりとりを行う。

【0086】

よって、上記第3の問題点とされていた、衛星回線のみをデータ伝送システムに組み込むことによる弊害、例えば、情報が各データ受信装置に正しく伝わった

かどうかをデータ送信装置が知ることができない等といった問題を解決することができる。

【0087】

また、データ送信装置2からデータ受信装置3へのセッション鍵Ksの伝送については、片方向通信経路とされる衛星回線4aに行ってもよく、双方向の通信経路9によって行っててもよい。

【0088】

セッション鍵Ksの更新手順については、図4に示すようなフローチャートに従って実行される。

【0089】

まず、ある時点において、データ受信装置3は、セッション鍵Ks34として、セッション鍵Ks_evenと、セッション鍵Ks_oddの2つを保持している。データ受信装置3は、このようにセッション鍵Ksを2つ所持することにより、このセッション鍵Ks_even又はセッション鍵Ks_oddの何れかを使用して、データ送信装置2から送信されてくる情報データの復号化を行う。

【0090】

ここで、現在使っているセッション鍵Ksがどちらであるかは、上記図2に示すセッションヘッダ部103に情報として書き込まれている。例えば、セクションヘッダ部103は、図5に示すように、テーブルID(table_id)、MACアドレス部(MAC_address_1, MAC_address_2, MAC_address_3, MAC_address_4, MAC_address_5, MAC_address_6)と、セクション情報部(section_length, section_number, last_section_number)、ssi(section_syntax_indicator)、pi(private_indicator)、rsvd(reserved)、psc(payload_scramble_indicator)111、asc(address_scramble_indicator)、Lsf(LLC_SNAP_flag)及びcni(current_next_indicator)によって構成されている。ここで、psc111が現在使っているセッション鍵Ksがどちらであるかの情報を示す。例えば、上記psc111は、2ビットの情報であり、例えば、pscの上位ビットが「0」のときは、セッション鍵Ks_evenが使用されていることを示し、pscの下位ビットが「1」のときには、セッション鍵Ks_oddが使用されていること

を示す。

【0091】

上述したような使用されているセッション鍵Ksの判断をステップS1において行った後、データ受信装置3は、ステップS2において、タイマーでトリガをかけ、セッション鍵Ksの更新タイミングを知る。

【0092】

続いて、データ受信装置3は、ステップS3において、MACアドレスとセッション鍵Ksの対応表にある現在のセッション鍵Ksのフラグを更新する。データ受信装置3は、例えば、図6のMACアドレスとセッション鍵Ksの対応表を有しており、この対応表を参照して、現在のセッション鍵Ksのフラグ112を更新する。この更新処理により、上記のpsc111の上位1ビットが反転する。例えば、pscの上位ビットが「0」に反転される。

【0093】

そして、データ受信装置3では、ステップS4において、そのpscに基づいてそのセクションに含まれているIPデータグラムの復号化を行う。すなわち、pscの上位ビットが「0」とされた場合には、データ受信装置3は、これまで使用していたセッション鍵Ks_odd (pscの上位ビットが「1」のとき使用されるセッション鍵Ks) から変更して、セッション鍵Ks_evenにより復号化を行う。また、pscの上位ビットが「1」とされた場合には、データ受信装置3は、これまで使用していたセッション鍵Ks_even (pscの上位ビットが「0」のとき使用されるセッション鍵Ks) から変更して、セッション鍵Ks_oddにより復号化を行う。

【0094】

そして、次のセッション鍵Ksの切替えのタイミングまでの間に、ステップS5において、データ送信装置2からデータ受信装置3に対して、次のセッション鍵Ksをマスター鍵Km24により暗号化して転送する。

【0095】

ここで、暗号化されたセッション鍵Km(Ks)の転送は、衛星回線4a又は双方の通信回線9を使って伝送する。例えば、伝送の際のプロトコルについては、

応答の伴うプロトコルを用い、例えば、TCP/IP (Transmission Control Protocol / Internet Protocol) を使用する。これにより、データ送信装置2からデータ受信装置3へのセッション鍵Ksの伝送が確実に行われる。

【0096】

そして、この転送処理の間に、ステップS6において、データ受信装置3は、図6に示すMACアドレスのセッション鍵Ksの対象表の更新を行う。すなわち、以前使用していたセッション鍵Ksを、新しいセッション鍵Ksに書き換える処理を行う。

【0097】

その後、ステップS7において、データ受信装置3は、対象とするデータ受信装置3に次のセッション鍵Ksが保持されたかを確認した後に、ステップS8に進み、次のセッション鍵Ksに切り替える。ここで、ステップS8以降ステップS13までの処理は、pscの上位ビットが「1」とされて、セッション鍵Ks_oddを復号化に使用するときの処理であって、上記ステップS7から進む処理であり、また、上記ステップS1において、データ受信装置3が現在のセッション鍵Ksがセッション鍵Ks_even (pscの上位ビットが「0」)とされたときに実行される処理である。

【0098】

上述したような手順により、データ送信装置2は、確実に更新されるセッション鍵Ksをデータ受信装置3に届けることができ、データ受信装置2では、2つ所持するセッション鍵Ksを切替えを瞬時に行い、データの取りこぼしもなくセッション鍵Ksによる復号化を実現することができる。なお、伝送処理時間の許す範囲で、セッション鍵Ks24の更新頻度は柔軟に変更することが可能である。

【0099】

以上のようにセッション鍵Ksがデータ受信装置3において、逐次変更されている。データ受信装置3は、このように変更されるセッション鍵Ksによって、共に転送されてくる情報データの復号を行っている。

【0100】

次にデータ送信装置2がデータを送信するまでの手順、及びデータ受信装置が

データを受信したときの手順について説明する。データ送信装置2がデータを送信するまでの手順については、例えば、図7に示すフローチャートに従って実行している。そして、データ受信装置3がデータを受信してからの手順については、例えば、図9に示すフローチャートに従って実行している。

【0101】

先ず、データ送信装置2がデータを送信するまでの手順については、ステップS21において、データ送信装置2は、データ受信装置3に伝送するIPデータグラムを、データ送信装置2自身又は双方向の通信経路9に繋がるインターフェースより、受け取る。インターネット6上からのアクセス情報に基づいて、情報センタの情報の提供を受け取る。

【0102】

次にステップS22において、データ送信装置2は、IPデータグラムの宛先アドレスを見て、第1のプロトコルの宛先アドレスを知る。例えば、データ送信装置2は、当該データ送信装置2内に所持している図8に示すようなIPアドレスとMACアドレスの対応表からデータ受信装置3の第1のプロトコルでの宛先アドレスを知る。

【0103】

そして、宛先アドレスを知ったデータ送信装置2は、その宛先アドレスをもとに上記セクションを作成する。ここで、データ送信装置2は、必要に応じてデータ部にビット1によるパディングを行い、データ部が64ビットの倍数になるようとする。

【0104】

次に、ステップS23において、例えば図6に示すようなMACアドレスとセッション鍵Ksの対応表から現在のセッション鍵Ksのフラグ112を見て、現在使用しているセッション鍵Ks24を取り出し、当該取り出したセッション鍵Ksにより、上記図2中(c)に示すように、セクションのデータ部を暗号化する。その際、現在のセッション鍵Ksのフラグを見て、その内容を上記図6に示すセッションのヘッダ部のpsc111の上位1ビットに入れる。

【0105】

次にステップS24において、図2中(e)乃至図2中(g)に示すように、このセクション全体109を分割して各TSパケット106, 107, 108のペイロード部Pに入れ、当該TSパケット106, 107, 108に予め定められた上記PIDを付加し、さらに、第2のプロトコルの必要に応じてペイロード部Pを暗号化し、衛星回線4aに送出する。

【0106】

以上がデータ送信装置2がデータを送信するまでの手順である。そして、データ受信装置3では、上述のようにして衛星回線4aに送出されたデータを受信する。

【0107】

データ受信装置3は、先ず図9のステップS31において、衛星回線4aより受信したTSパケット106, 107, 108を第2のプロトコルに従って復号化し、セクション全体109を再構築する。

【0108】

次に、ステップS32において、データ受信装置3は、セクションの宛先アドレス(MACアドレス)を取り出し、続いて、ステップS33において、図10に示すMACアドレスとセッション鍵Ksの対応表を参照してMACアドレスが存在するか否かの判別処理を行う。すなわち、自己に送信が許可されているデータを格納しているものであるか否かの判別処理を行う。ここで、MACアドレスがないことを確認した場合には、データ受信装置3は、ステップS34に進み、そのデータの破棄の処理を行う。また、MACアドレスがあることを確認した場合には、データ送信装置3は、ステップS35に進み、セクションヘッダ部103より上記図5に示すpsc111を取り出す。そして、データ送信装置3は、そのpsc111の上位1ビットから現在有効なセッション鍵Ksがどちらであるかを調べ、2つのセッション鍵Ksから現在有効とされるセッション鍵Ksを取り出す。

【0109】

データ受信装置3は、このようにして取り出したセッション鍵Ksにより、ステ

ップS36において、セクションデータ部104をTriple-DESにより復号化する。そして、データ受信装置3は、ステップS37において、当該復号したデータからIPデータグラムを取り出す。例えば、IPデータグラムの取り出しは、復号化されたデータ部の先頭にあるIPヘッダから図11のTOTAL LENGTHフィールド113を読み取り、IPデータグラムの長さを調べ、そこから計算されるIPデータグラム全体を取り出す。これにより、暗号化の際に付加した余計なパディングを除去される。このようにして目的とするIPデータグラムを取り出すことができる。

【0110】

以上のような手順により、データ送信装置2は、データを送信するまでの処理を行い、また、データ受信装置3は、受信したデータに対する処理を行い、自己に宛てて配信されてきた情報データを受け取る。

【0111】

このように構成されたデータ伝送システム1は、上述したように、各問題を解決することができる。

【0112】

なお、上記データ伝送システム1は、次のように変形することができる。第1の変形例であるデータ伝送システム201は、図12に示すように構成される。このデータ伝送システム201は、データ受信装置3がIPルータとして構成される場合である。

【0113】

ところで、上述したデータ伝送システム1では、データ受信装置3aが直接IPデータグラムを受信する構成としている。しかし、このデータ伝送システム201では、データ受信装置3aをIPルータとして構成することにより、データ受信装置3aが衛星回線4aから受信したデータを、イーサネットなどのローカルエリアネットワーク(LAN)202を経由してつながっている衛星回線4aへのインターフェースを持たないコンピュータ203a, 203bにもデータを伝送することができる。その際、データ送信装置2やデータ受信装置3aは、データ受信装置3aだけでなく、それがつながっているローカルエリアネットワー

ク202上のコンピュータ203a, 203b全てについてのデータの限定受信制御を行うことができるようになる。具体的には、図8に示すデータ送信装置2内のIPアドレスとセクションの宛先アドレス(MACアドレス)の対応表のIPアドレスが、個別のIPアドレスではなく、複数のIPアドレスの集合を示すIPのネットワークアドレスに変わることになる。但し、データ伝送システム201において、データ伝送を行うのは衛星回線4aの区間のみであるため、データ受信装置3aとコンピュータ203a, 203bとの間でもデータ限定伝送制御を行うには、IPプロトコル又はそれより上位のアプリケーションのレベルでのデータ限定伝送制御が必要となる。

【0114】

第2の変形例であるデータ伝送システム301は、図13に示すように構成されている。このデータ伝送システム301では、データ受信装置3aがブリッジとして構成され、IPデータグラムを伝送するプロトコルの変換のみを行い、上記データ伝送システム201とでは、ルーティングを行わないことで異なる。

【0115】

上記データ受信装置3aは、衛星回線4aより受信したデータを復号化してIPデータグラムを取り出し、それをイーサネットフレームに入れて汎用のルータ302に転送する。そして、汎用のルータ302が、通常のIPデータグラムに対する処理を行う。これにより、ルーティングを行わないとためにデータ受信装置3aの構成が簡単になり、既存の汎用のルータを用いることができるようになる。

【0116】

【発明の効果】

本発明に係るデータ伝送制御方法は、データ送信手段からデータ受信手段へのデータの伝送に使用する第1の通信経路を介して、データ送信手段からデータ受信手段へのデータの送信を行い、第1の通信経路よりもデータ伝送容量の小さく、データ受信手段からデータ送信手段へのデータの伝送にも使用される第2の通信経路、及び第1の通信経路の内の少なくとも第2の通信経路を介して、データ送信手段及びデータ受信手段の間でデータ限定伝送制御情報の送信を行うことが

できる。

【0117】

このデータ伝送制御方法により、第1の通信経路及び第2の通信経路によりデータ送信手段からデータ受信手段へのデータ限定伝送制御情報を含むデータの送信を行うとともに、第2の通信経路により当該データ送信手段と当該データ受信手段との間でのデータの送受信に関する情報に関して情報の交換を行うことができる。

【0118】

よって、例えば、情報が各データ受信手段にデータが正しく伝わったかどうかをデータ送信手段が知ることができるようになる。

【0119】

本発明に係るデータ伝送システムは、データ送信手段からデータ受信手段へのデータの伝送に使用する第1の通信経路を介して、データ送信手段からデータ受信手段へのデータの送信を行い、少なくともデータ送信手段からデータ受信手段へのデータの伝送にも使用される通信経路であって、第1の通信経路よりもデータ伝送容量の小さい第2の通信経路を介して、データ送信手段及びデータ受信手段の間でデータ限定伝送制御情報の送信を行うことができる。

【0120】

これによりデータ伝送システムは、第1の通信経路及び第2の通信経路によりデータ送信手段からデータ受信手段へのデータ限定伝送制御情報を含むデータの送信を行うとともに、第2の通信経路により当該データ送信手段と当該データ受信手段との間でのデータの送受信に関する情報に関して情報の交換を行うことができる。

【0121】

よって、例えば、情報が各データ受信手段にデータが正しく伝わったかどうかをデータ送信手段が知ることができるようになる。

【0122】

また、本発明に係るデータ伝送制御方法は、データ送信手段からデータ受信手段に送信されるデータが複数のプロトコルによって多重化してカプセル化できる

【0123】

これにより、所定のプロトコルを保ったままデータの送信が可能になり、すなわち、例えば、所定のプロトコルとの互換性を保ったままデータの送信が可能になり、さらに、所定のデータを格納するための空間が確保することができるプロトコルによりカプセル化することにより、各種情報を格納するためのデータ空間を確保することができる。さらに、暗号化が施されることにより、データの安全性を保することができる。

【0124】

例えば、所定のデータを収納することができるプロトコルによってカプセル化することにより、暗号鍵等の宛先アドレスに関する情報を格納するための空間を十分に確保することができ、従来のTSパケット方式を採用したときにPID部及びスクランブル制御部に格納していたときよりも宛先アドレスに関する情報を増加させることができる。これにより、PID部を増加させなくて済む。

【0125】

また、例えば、アプリケーション毎に制御方法を用意しなくて済み、新しいアプリケーションへの素早い対応ができるようになる。また、認証ヘッダや暗号ペイロードを既存のインターネットで使うことができるようになる。

【0126】

また、本発明に係るデータ伝送制御方法は、データ暗号工程において暗号鍵により暗号化されたデータに当該データの暗号化に使用した暗号鍵に関する暗号鍵情報を附加して、データ送信工程により、データ送信手段からデータ受信手段へ当該データを送信することができる。そして、データ受信手段において、データ復号化工程により、受信した暗号化されたデータを復号するための複数の復号鍵であって、頻繁に更新される復号鍵から、暗号化されたデータに付加されている暗号鍵情報に基づいて選択した一つの復号鍵により、当該暗号化されたデータの復号化を行うことができる。

【0127】

このデータ伝送制御方法により、データ送信手段は、暗号鍵によるデータの暗

号化を行い、データ受信手段は、受信した暗号化されているデータを復号鍵により復号化することができる。さらに、データ受信手段は、頻繁に変更される復号鍵から一つの復号鍵を選択して、当該選択した復号鍵により復号化を行うことができる。このとき、データ受信手段は、当該暗号化されたデータとともに送信されてくる暗号鍵情報に基づいて複数の復号鍵から一つの復号鍵を選択する。

【図面の簡単な説明】

【図1】

本発明の実施の形態であるデータ伝送システムの構成を示す図である。

【図2】

上記データ伝送システムを構成するデータ送信装置からデータ受信装置へ送信されるデータであって、複数のプロトコルによってカプセル化が施されたデータを示す図である。

【図3】

上記データ送信装置及び上記データ受信装置の構成を示すブロック図である。

【図4】

上記データ送信装置から上記データ受信装置へ送信されるデータを暗号化するセッション鍵の変更を行う手続きの一連の工程を示すフローチャートである。

【図5】

セクションヘッダのデータ構造を示す図である。

【図6】

MACアドレスとセッション鍵Ksのフラグとの対応表を示す図である。

【図7】

上記データ送信装置において行うデータのカプセル化の一連の手続きを示すフローチャートである。

【図8】

IPアドレスとMACアドレスとの対応表を示す図である。

【図9】

上記データ受信装置が受信したデータをセッション鍵Ksにより復号化するときの一連の手続きを示すフローチャートである。

【図10】

MACアドレスとセッション鍵Ksの対応表を示す図である。

【図11】

IPデータグラムの取り出しの際に使用されるTOTALLENGTHフィールドが格納されるデータ構造を示す図である。

【図12】

上記データ伝送システムの第1の変形例を示す図である。

【図13】

上記データ伝送システムの第2の変形例を示す図である。

【図14】

従来のデータ伝送システムの構成を説明するために用いた図である。

【図15】

上記従来のデータ伝送システムにおいてデータを伝送するためのイーサネットフレームのデータ構造であって、宛先アドレスが格納されているイーサネットフレームのデータ構造を示す図である。

【図16】

従来のデータ伝送システムにおいて、イーサネットを介して受信したイーサフレームに自己の宛先アドレスが格納されているか否か、さらにその判断に基づいて行う処理についての一連の手続きを示すフローチャートである。

【図17】

T Sパケットのデータ構造のフォーマットを示す図である。

【図18】

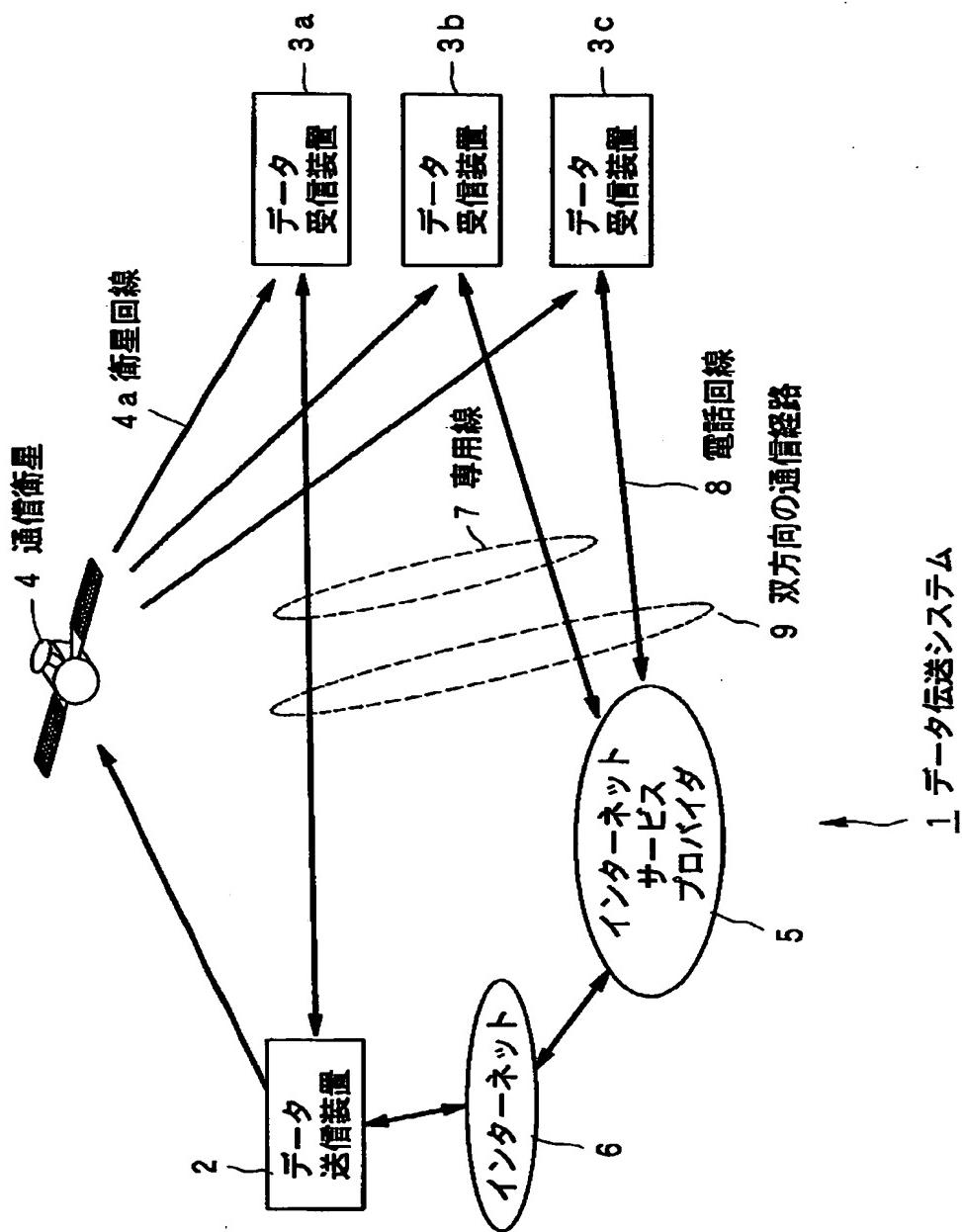
従来のデータ伝送システムを構成するデータ送信装置及びデータ受信装置の構成を示す図である。

【符号の説明】

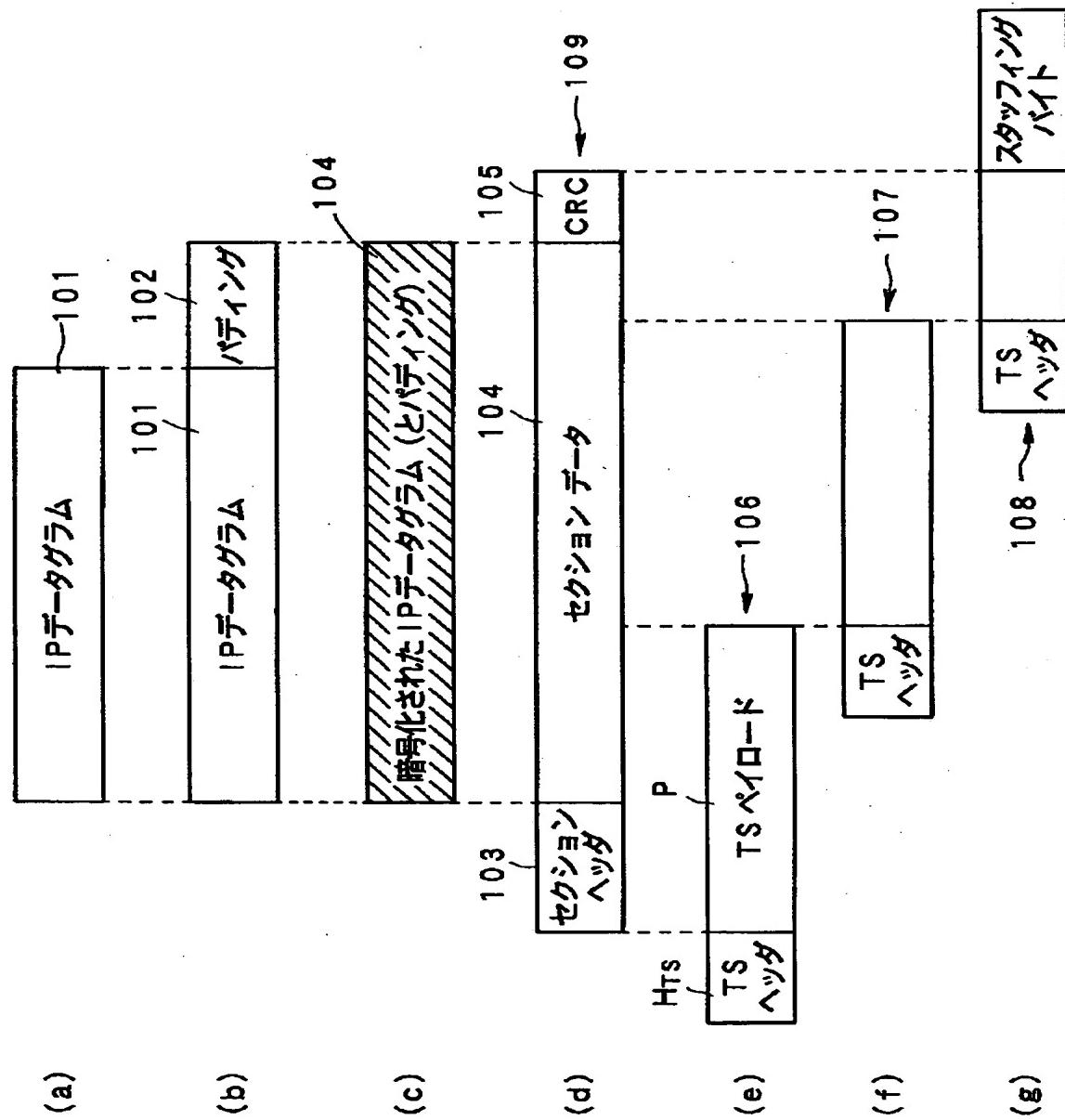
1 データ伝送システム、2 データ送信装置、3 データ受信装置、4
通信衛星、4 a 衛星回路、7 専用線、8 電話回線、9 双方向の通信回線
、24 セッション鍵、25 マスター鍵

【書類名】 図面

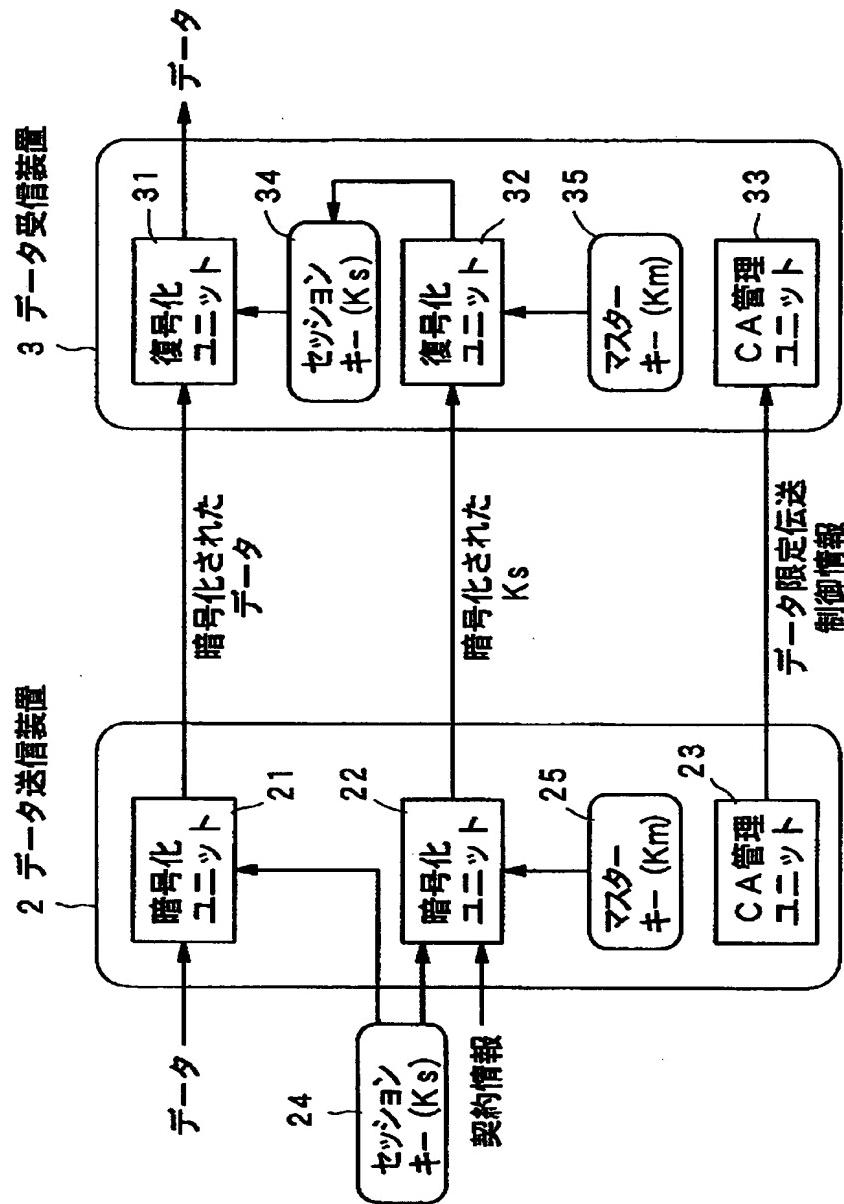
【図1】



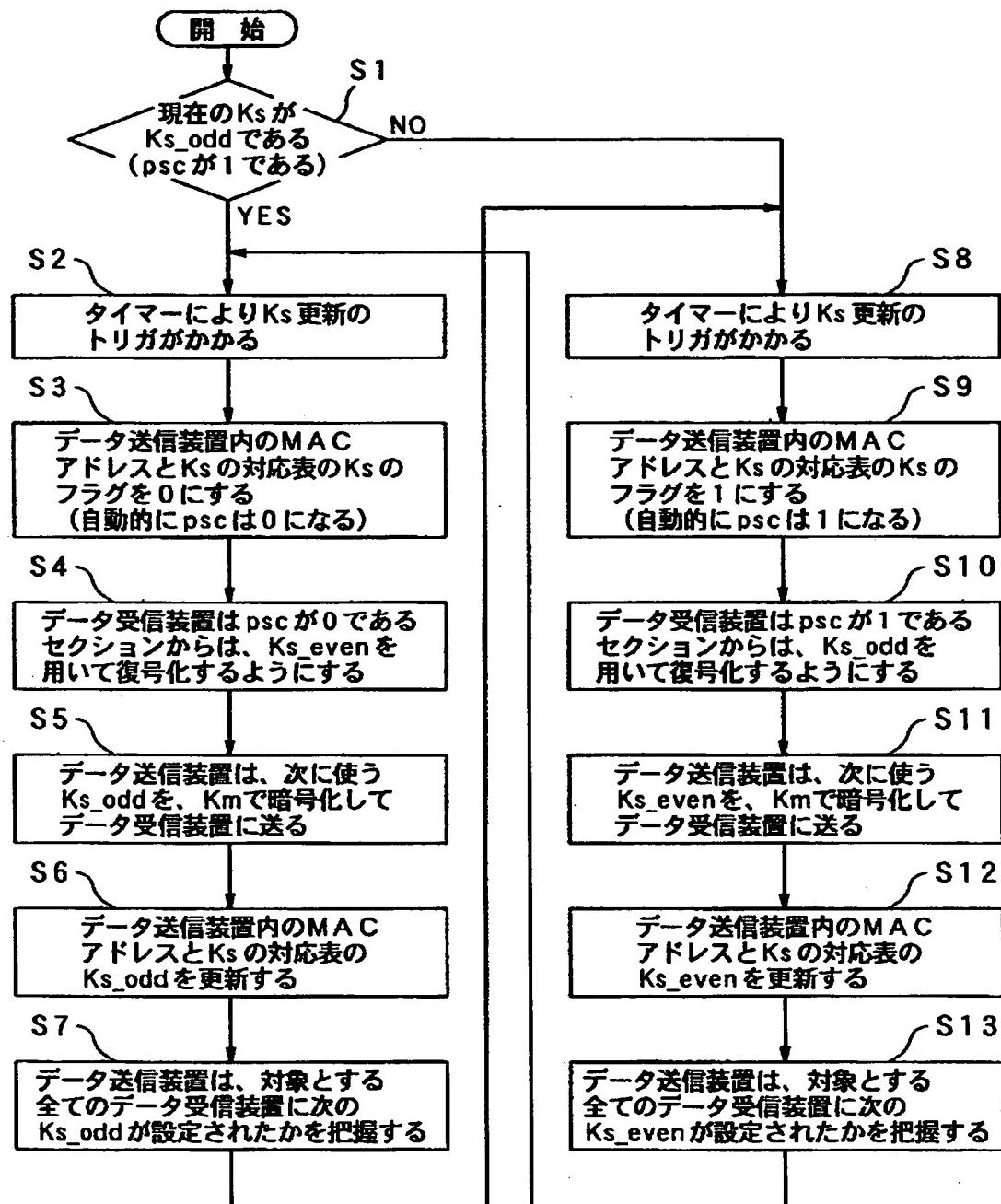
【図2】



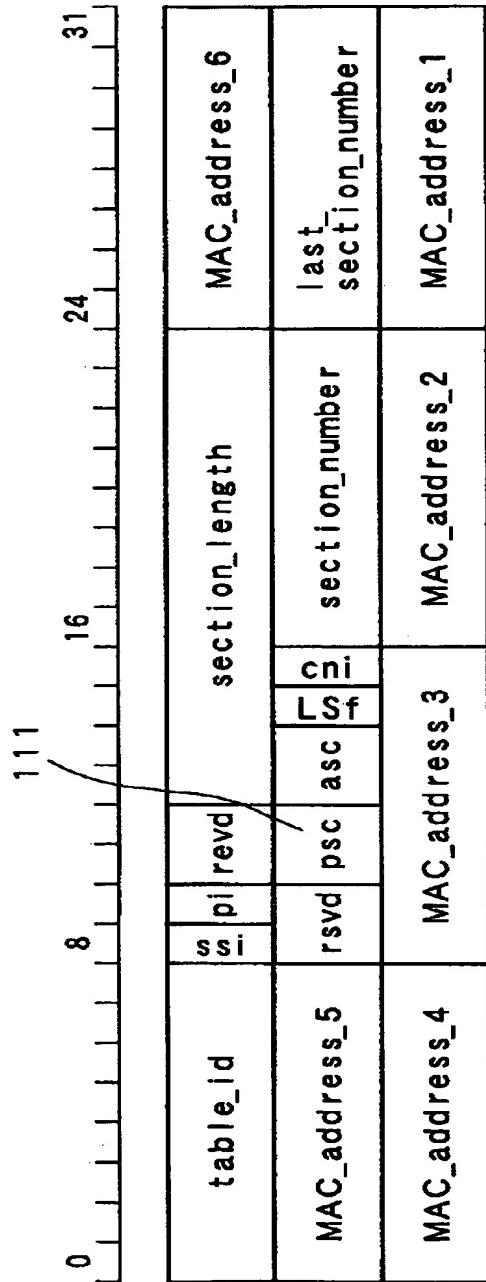
【図3】



【図4】



【図5】



```

ssi : section_syntax_indicator
pi  : private_indicator
rsvd : reserved
psc : payload_scramble_indicator
asc : address_scramble_indicator
LSf : LLC_SNAP_flag
cni : current_next_indicator

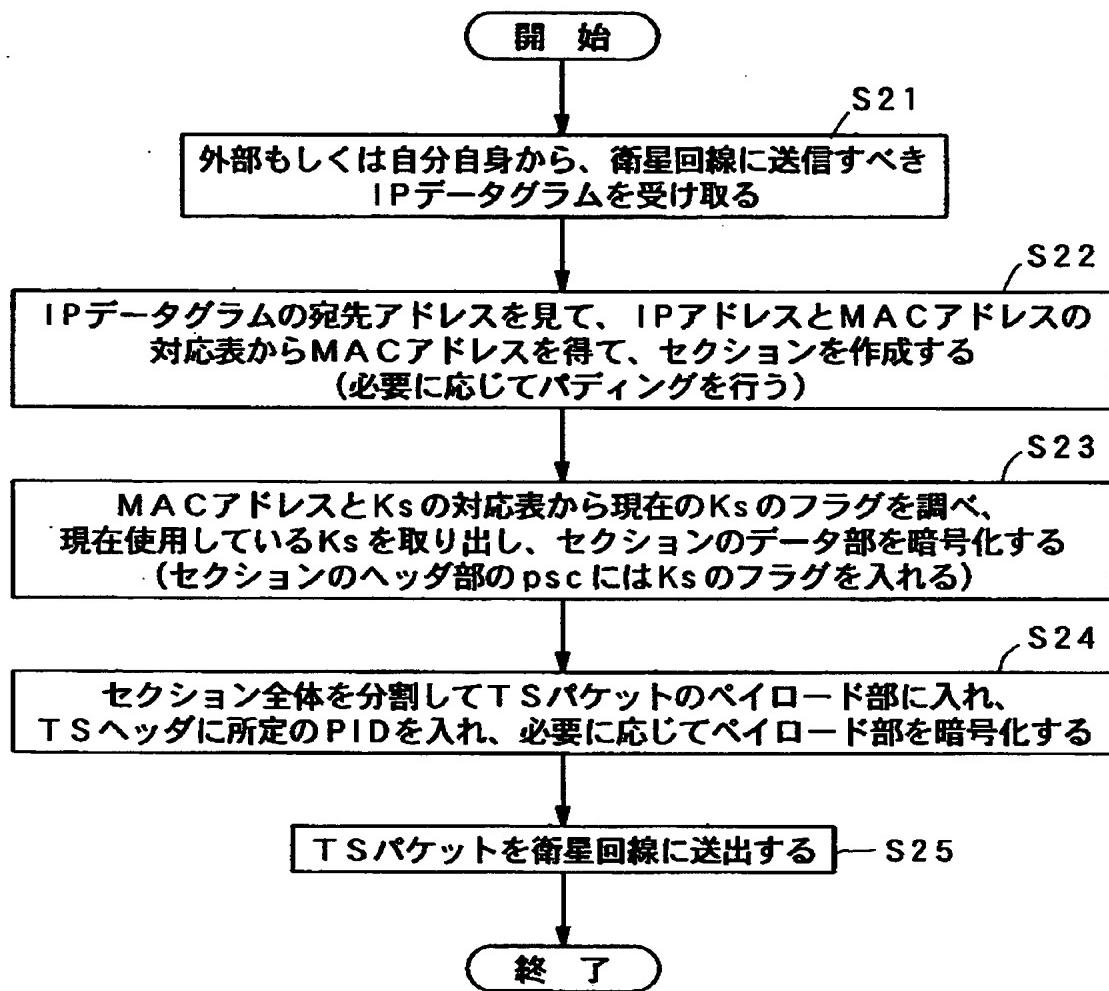
```

【図6】

112
/

MACアドレス	Ks_even	Ks_odd	Ksフラグ
08:00:46:01:07:24	0xC08F... 25	0x90B3... AF	0
08:00:46:01:07:09	0x26D2... 61	0xBA02... 3C	1
01:00:5e:16:0:0	0x461E... 67	0xDC1A... 22	0

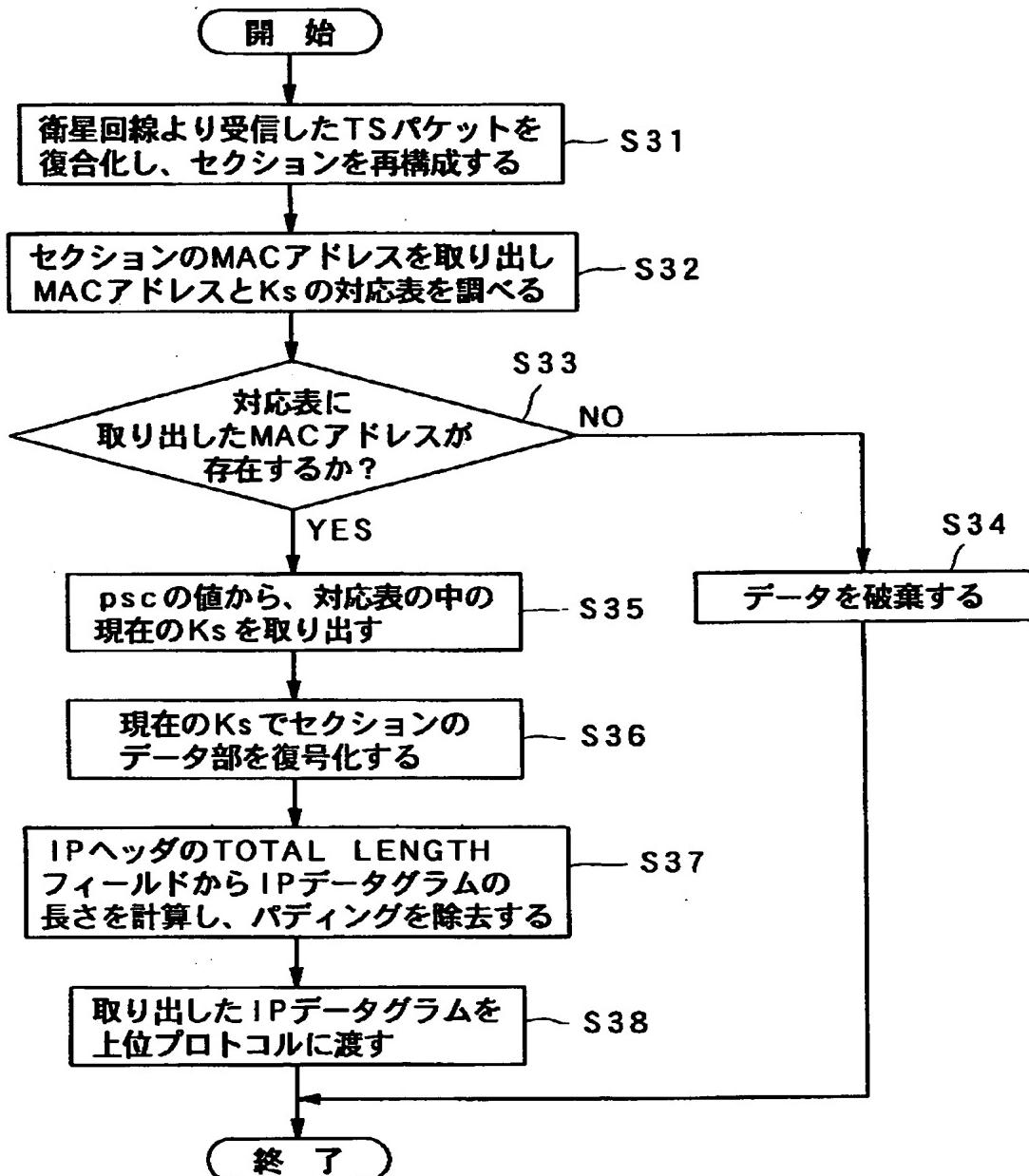
【図7】



【図8】

IPアドレス	bitmask	MAC address
133.11.9.39	255.255.255.225	08:00:46:01:07:24
133.11.20.0	255.255.255.0	08:00:46:01:07:09
226.0.0.0	255.255.255.224	01:00:5e:16:0:0

【図9】



【図10】

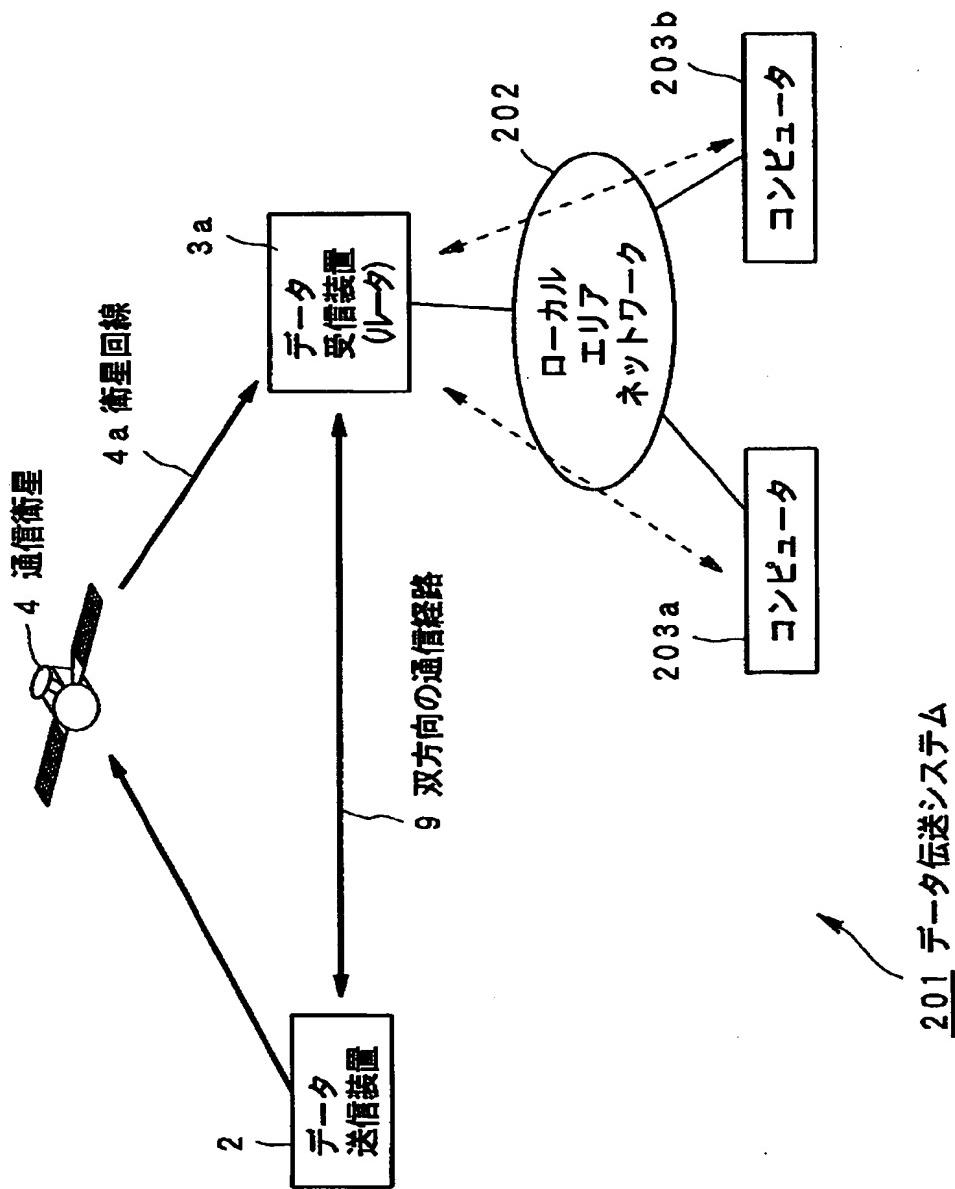
MACアドレス	Ks_even	Ks_odd
08:00:46:01:07:24	0xC08F...25	0x90B3...AF
01:00:5e:16:0:0	0x461E...67	0xDC1A...22

【図11】

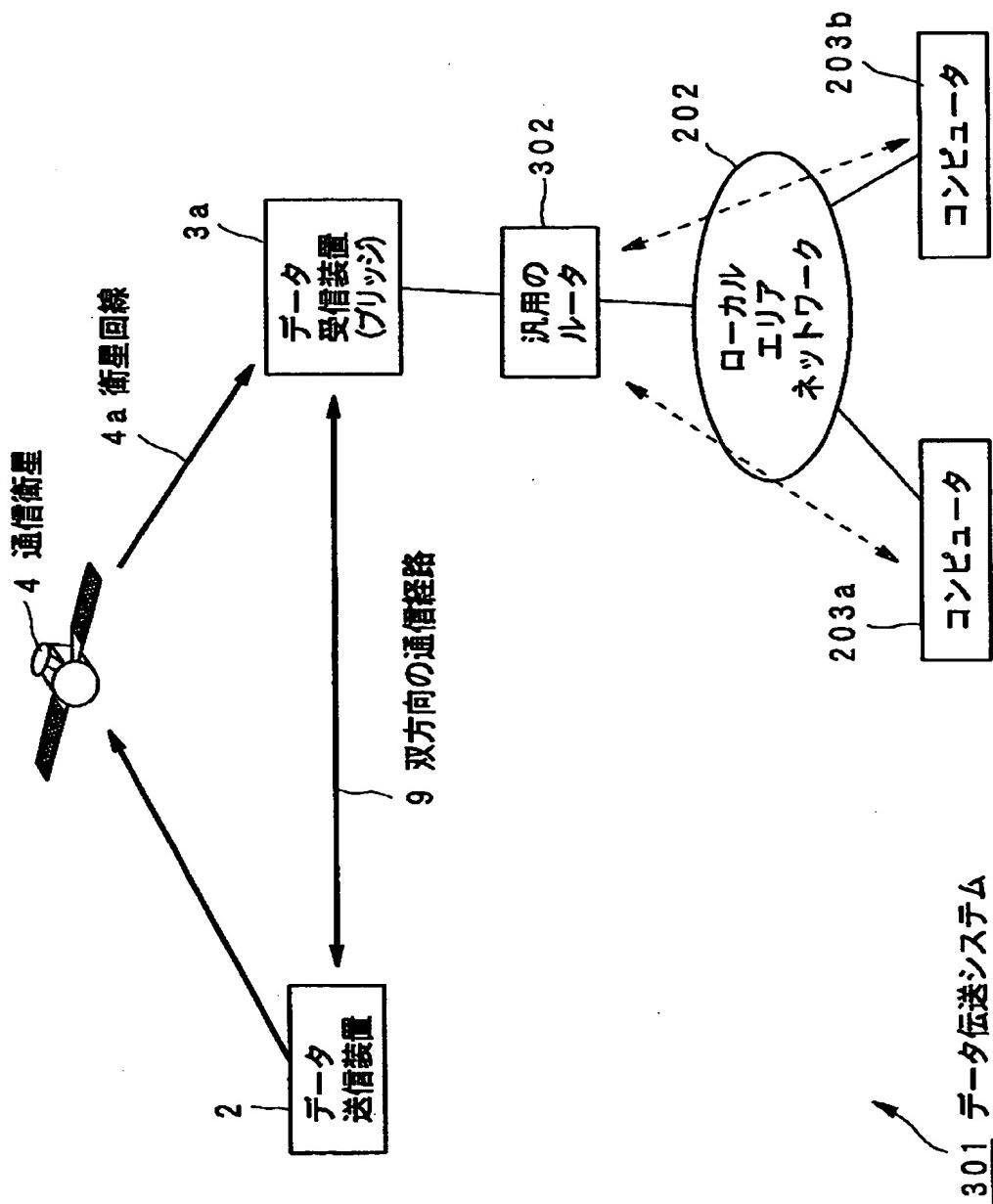
113

VERS	HLEN	SERVICE TYPE	TOTAL LENGTH	
IDENTIFICATION		FLAGS	FRAGMENT OFFSET	
TIME TO LIVE	PROTOCOL	HEADER CHECKSUM		
SOURCE IP ADDRESS				PADDING
DESTINATION IP ADDRESS				DATA
IP OPTIONS (IF ANY)			

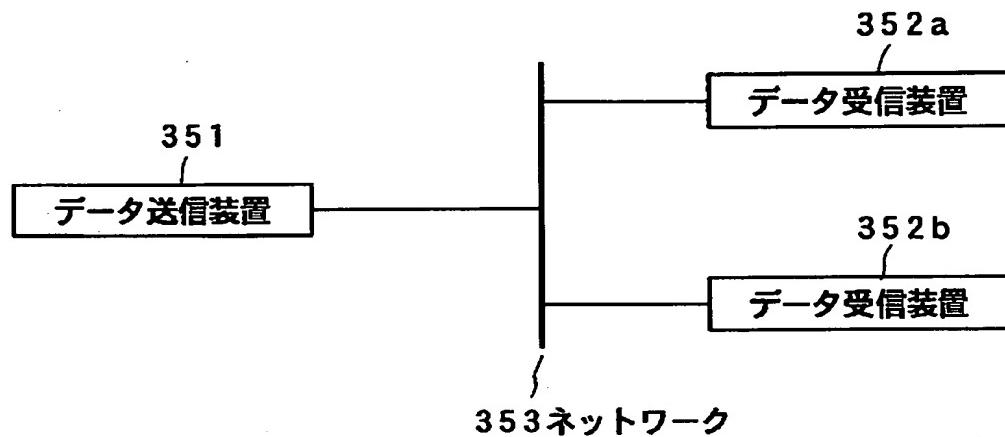
【図12】



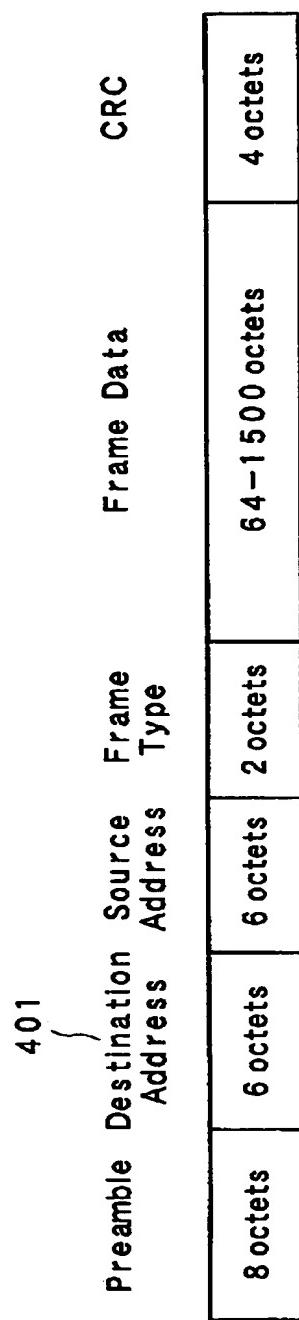
【図13】



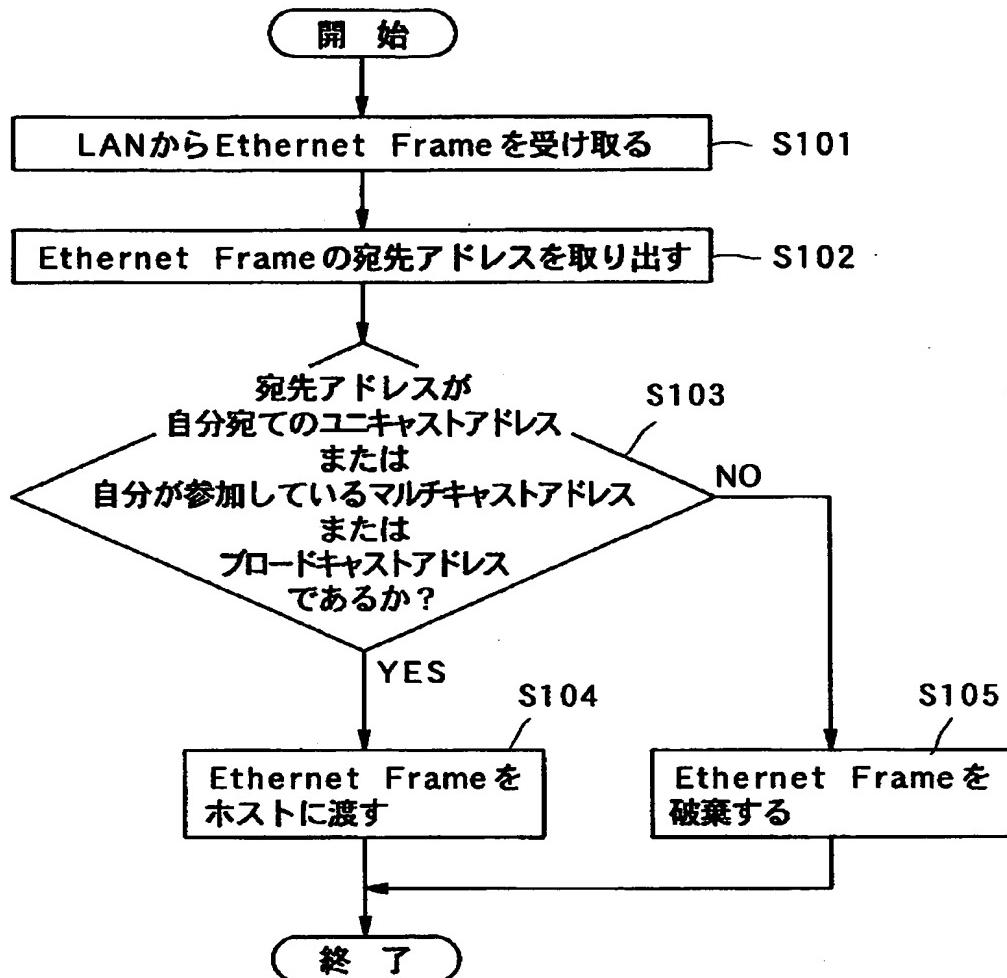
【図14】



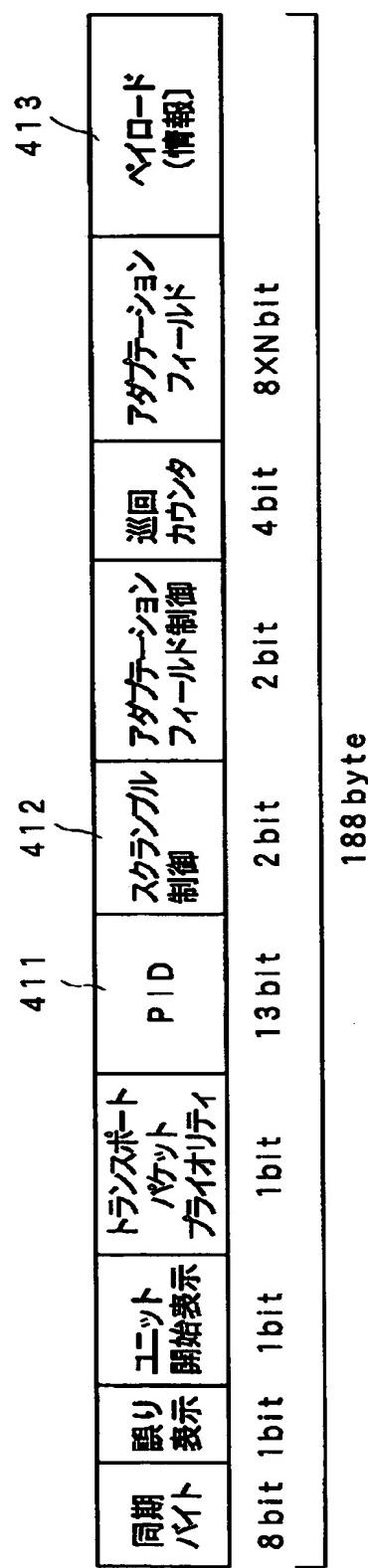
【図15】



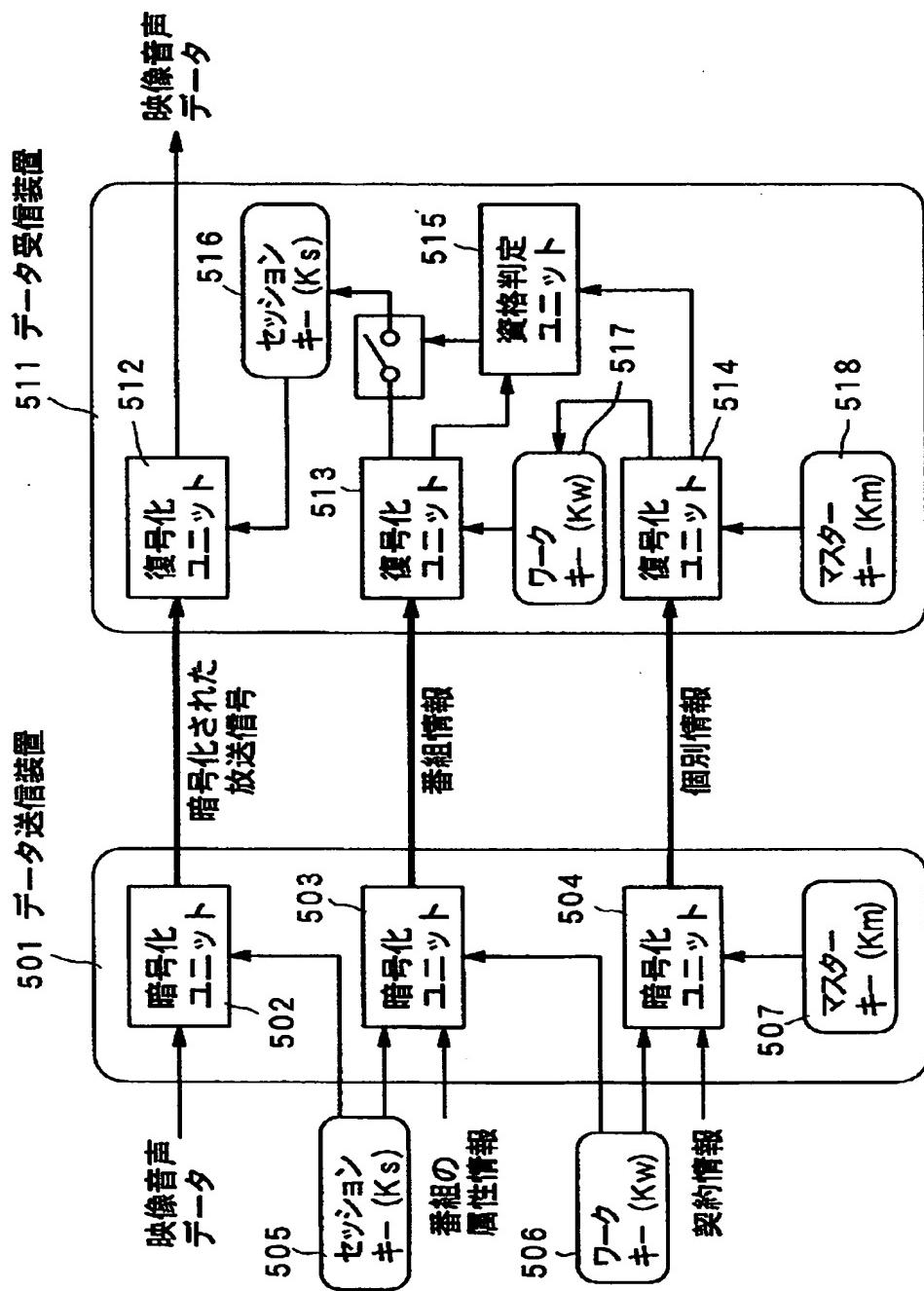
【図16】



【図17】



【図18】



【書類名】 要約書

【要約】

【課題】 データ送信装置からデータ受信装置へのデータの送信を安全に、さらに確実に行うことの実現可能にするデータ伝送システムの提供を目的とする。

【解決手段】 データ伝送システム1は、暗号化を施してデータを送信するデータ送信装置2と、データ送信装置2から暗号化が施されたデータが配信されるデータ受信装置3a, 3b, 3cと、データ送信装置2からデータ受信装置3a, 3b, 3cへのデータの伝送に使用する衛星回線4aと、データ受信装置3a, 3b, 3cからデータ送信装置2へのデータの伝送にも使用され、衛星回線4aよりもデータ伝送容量の小さい双方向の通信経路9とを有し、データ送信装置2からデータ受信装置3a, 3b, 3cへの暗号化したデータの伝送には、衛星回線4aを用い、データ送信装置2とデータ受信装置3a, 3b, 3cとの間のデータ限定伝送制御情報の通信には、少なくとも双方向の通信経路9を用いる。

【選択図】 図1

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000002185
【住所又は居所】 東京都品川区北品川6丁目7番35号
【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100067736
【住所又は居所】 東京都港区虎ノ門2-6-4 第11森ビル 小池
【氏名又は名称】 国際特許事務所
小池 晃

【選任した代理人】

【識別番号】 100086335
【住所又は居所】 東京都港区虎ノ門2丁目6番4号 第11森ビル
【氏名又は名称】 小池国際特許事務所
田村 篤一

【選任した代理人】

【識別番号】 100096677
【住所又は居所】 東京都港区虎ノ門二丁目6番4号 第11森ビル
【氏名又は名称】 小池国際特許事務所
伊賀 誠司

出願人履歴情報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社